Збірник матеріалів

Світ інформації та телекомунікацій

III Міжнародна науково-технічна конференція студентства та молоді

26 грудня 2016 р.

Міжнародний союз електрозв'язку
Державний університет телекомунікацій
Студентська рада Державного
університету телекомунікацій
Наукове товариство студентів та аспірантів
Державного університету телекомунікацій

«СВІТ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ»

Збірник матеріалів

III Міжнародної науково-технічної конференції студентства та молоді

26 грудня 2016 р.

КИЇВ

«Світ телекомунікацій та інформатизації»: матеріали ІІІ Міжнародної науково-технічної конференції студентства та молоді. – Київ: ДУТ, 2016 – 352 с.

Збірник містить матеріали ІІІ Міжнародної науково-технічної конференції студентства та молоді «Світ інформації та телекомунікацій». Пропонує статті та тези студентів й аспірантів, що висвітлюють перспективи розвитку інформаційних та телекомунікаційних технологій в Україні та світі.

Упорядники:

Похабова Ірина Едуардівна, начальник відділу з питань соціальних та навчальних проблем студентів Державного університету телекомунікацій.
Бондаренко Євгеній Олександрович, голова Студентської ради Державного університету телекомунікацій.
Школьний Іван Олександрович, голова Студентської ради факультету Телекомунікацій Державного університету телекомунікацій.
Щетініна Анастасія Артурівна, голова Студентської ради факультету Інформаційних технологій Державного університету телекомунікацій.
Приходько Владислав Олександрович, голова Студентської ради Навчально-наукового інституту Захисту інформації Державного університету телекомунікацій.
Кравченко Родіон Миколайович, голова Студентської ради Навчально-наукового інституту Менеджменту та Підприємництва Державного університету телекомунікацій.

Відповідальність за грамотність, автентичність цитат, правильність фактів та посилань несуть автори матеріалів

ЗМІСТ

Бондаренко Евгений Александрович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

САМООРГАНИЗУЮЩИЕСЯ СЕТИ SON

Стандарты самоорганизующихся сетей консорциум 3GPP начал разрабатывать еще в релизах 8 и 9, затем продолжил в релизе 10, который был закончен в июне 2011 года. Релиз 11, посвященный LTE-A, также охватывает дополнительные функции и расширения SON (Self-Organizing Network).

Основными мотивами введения архитектуры SON были естественные желания операторов сокращать (хотя бы не увеличивать) операционные расходы за счет уменьшения степени человеческого вмешательства на этапе планирования, внедрения и эксплуатации своих сетей, снижать капитальные затраты за счет оптимизации использования своих сетевых ресурсов, сохранять и наращивать прибыль, сокращая ошибки из-за человеческого фактора.

Существенную роль в достижении этих трех целей играет эксплуатационное управление OAM&P, объединяющее управление ресурсами (Operations), административное управление (Administration), техническое обслуживание (Maintenance) и ввод новых ресурсов (Provisioning). Если эти задачи непосредственно контролируются персоналом, даже со средствами автоматизации, этот ручной труд требует большого количества времени, значительных финансовых средств, высококлассных специалистов, и при этом человеческие ошибки все равно возможны. Разработка стандартов SON начата консорциумом 3GPP в релизе 8, затем продолжалась в релизах 9 и 10, а релиз 11 охватывает дополнительные функции и расширения SON (рис. 1).

Функция минимизация частоты использования мобильных тестирующих бригад MDT (Minimization of Drive Tests) на рис. 2. была описана в релизе 10 3GPP и относится к проблеме мобильных тестов. Такие тесты в сетях 1990-х и 2000-х реализовались с привлечением ручного труда персонала и потому являлись весьма дорогостоящими. Идея MDT базируется на результатах измерений, получаемых непосредственно от пользовательских устройств и содержащих информацию о местности, что позволяет иметь намного более глубокие знания о характеристиках пропускной способности соты, а также использовать эти знания для автоматизированных SON- функций.

Рис. 1. График работы 3GPP над стандартизацией SON

Развитие SON ориентируется на оптимизацию сети радиодоступа LTE, на минимизацию общих издержек на сетевую инфраструктуру SAE/LTE и ее эксплуатацию, на организацию хэндовера и на создание новых сценариев использования существующих и новых технологий. Использование SON для сокращения операционных расходов за счет уменьшения ручной работы и минимизации ошибок из-за человеческого фактора в эксплуатационном управлении OAM&P сети SAE/LTE иллюстрирует рис. 2.

Внедрение SON-функций позволяет минимизировать участие человека в эксплуатационных процедурах путем увеличения автоматизации сетевых элементов NE (Network Element), элементов управления доменом DM (Domain Management) или элементов управления сетью NM (Network Management).

На рис. 2. показано смещение от ручного планирования и конфигурации к мониторингу и управлению сетью средствами встроенной SON. Здесь человеческий фактор переводится на более высокий уровень управления, персонал сети освобождается от рутинных операций и вместо них занимается разработкой политик управления на уровнях сетевых элементов NE, управления элементами DM и управления сетью NM.

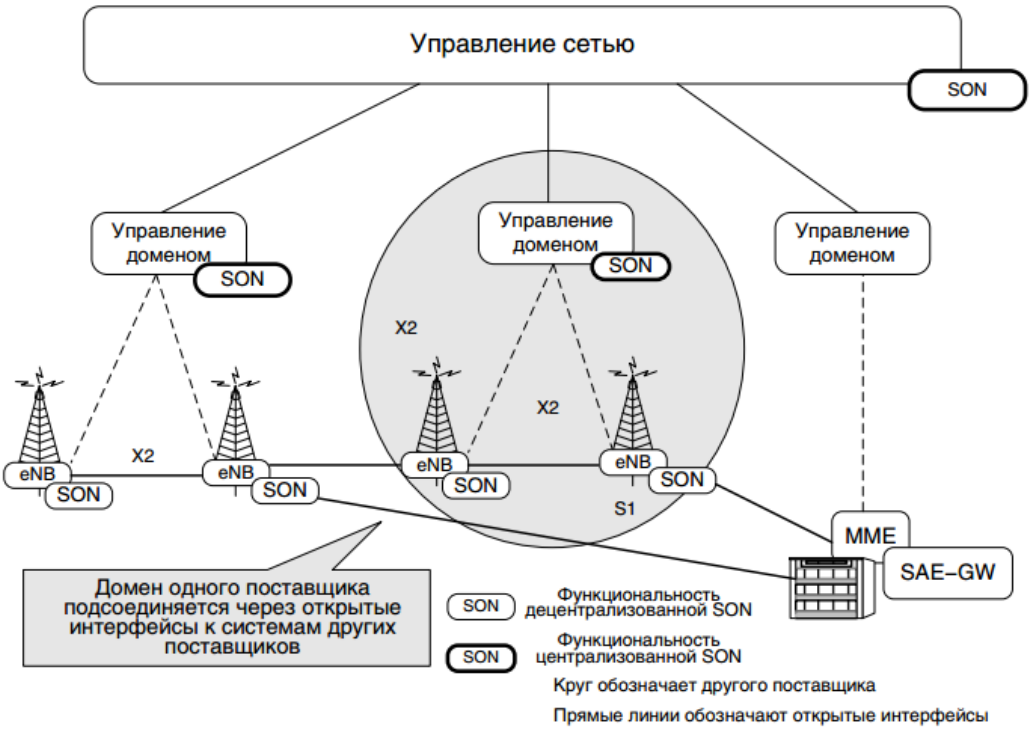


Рис. 2. Функции SON в архитектуре OAM&P консорциума 3GPP

На рис. 2 видно, что SON-функции располагаются на уровне управления сети NM (централизованная SON с использованием стандартных интерфейсов или интерфейсов от конкретного производителя), на уровне управления доменами DM (централизованная SON с использованием интерфейсов от конкретного производителя) и на уровне сетевых элементов NE (распределенная SON с использованием стандартных интерфейсов или интерфейсов от конкретного производителя, или местная SON, независимая от других и, следовательно, не требующая никаких интерфейсов). На всех этих уровнях в сети LTE выполняются основные группы функций SON:

- самоконфигурация – автоматическое переконфигурирование при реализации плана развертывания сети или при внедрении нового оборудования;
- самовосстановление – автоматическое обнаружение не-исправности и ее устранение;
- самооптимизация – автоматическое перераспределение задач между элементами сети с целью эффективного использования сетевых ресурсов, отказоустойчивости, балансировки нагрузки, энергоэффективности, оптимизация емкости и покрытия сети, оптимизация контроля интерференции между смежными сотами и др.

Например, пул узлов управления мобильностью MME может быть общим для всех eNodeB, находящихся под управлением в этой области пула (MME pool area), согласно в 3GPP TS23.401.

Для соседних базовых станций eNodeB средства SON могут перераспределять пользовательский трафик из более нагруженной соты к менее загруженной соседней соте за счет тех пользовательских устройств, которые находятся в области радиопокрытия обоих eNodeB. Т.е. SON может улучшить производительность сети, может разгрузить MME от части сигнальной нагрузки, может управлять перераспределением пользовательского трафика между сотами.

Это особенно эффективно в тех местах, где распределение пользователей по сотам изменяется во времени: спортивные соревнования, массовые мероприятия, автомобильные пробки. Но решение о балансировке сигнальной нагрузки между MME, входящими в один пул, или о хэндовере пользовательского устройства на смежную eNodeB для разгрузки обслуживающей eNodeB должно рассматриваться и относительно пользователя согласно принципу «не навреди». Т.е. SON не осуществляет вынужденный хэндовер пользовательского терминала к смежной соте, если это ухудшит качество обслуживания QoS или сократит пропускную способность новой соты для пользователя по сравнению с сотой, обслужившей его до хэндовера.

Для планирования сети LTE на самой начальной стадии требуются весьма профессиональные проектировщики, значительная трудоемкость и соответствующие финансовые затраты. При этом потребности пользователей в скорости передачи данных и условия окружающей среды обычно быстро изменяются, и, следовательно, возникает необходимость анализа новой ситуации в сети и в переконфигурировании базовых станций как LTE, так и эксплуатируемых совместно с LTE сетей 2.5G и 3G. Более того, стратегия поэтапного внедрения LTE предусматривает целесообразность использования не только макро-eNodeB, но и узких решений микро-eNB, пико-eNB и фемто-eNB, а также Wi-Fi точек доступа. То есть ситуация с переконфигурированием сот еще более усложнится за счет такого разнообразия и количества базовых станций.

Сложнее станут и мобильные тесты, которые даже сейчас являются достаточно дорогими. Целесообразно при этом расширять списки смежных сот за счет базовых станций, которые не являются смежными в данный момент, но находятся поблизости и могут быть потенциальными кандидатами на соседство. Но, во-первых, это ударит по энергопотреблению и без того слабых аккумуляторов современных пользовательских терминалов, т.к. абонентскому терминалу придется измерять уровень сигнала от канала BCCH большего числа базовых станций.

Во-вторых, это повысит количество неуспешных хэндоверов, увеличит вероятность прерывания речевых сеансов связи, снизит QoS. Поэтому для решения проблемы необходима оптимизация списков смежных сот. Оптимизированный, актуальный список соседств не только увеличит производительность каждой eNodeB и всего пула, но также улучшит пользовательское восприятие качества услуг и коэффициента готовности сети. Этого поможет достигнуть автоматическое установление соседских отношений средствами SON, позволяющее автоматизировать конфигурацию списка соседей каждой базовой станции.

Производительность сети тоже выигрывает от такой оптимизации и актуального списка соседств: например, соответствующая установка соседских отношений увеличит число успешных хэндоверов и уменьшит число обрывов связи из-за недостаточно актуального списка соседств. Именно для сети LTE/SAE с ее плоской архитектурой, без центральных узлов радиосети (например, без контроллеров базовых станций), необходимо конфигурировать большое число параметров соседств в каждой eNodeB всей сети. Притом делать это придется вручную, если не будет использоваться функция SON. Именно поэтому средства SON энергично разрабатываются и активно внедряются во всех разворачиваемых сегодня сетях 4G.

В заключение заметим, что строго говоря, технология LTE/SAE в том виде, в каком она появилась в релизах 8 и 9, не является технологией поколения 4G.

В литературе ее принято относить к поколению 3.9G, а к полноценному четвертому поколению относить только LTEAdvance начиная с версии релиза 10. Впрочем, это не более чем вопрос маркировки. Важно то, что LTE-Advance является все той же технологией LTE, равно как и то, что история эволюции на LTE-Advance отнюдь не заканчивается, про что авторы предполагают еще написать в будущем.

Література:

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E . Cayirci, “A survey on sensor networks” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.
2. S. S. Dhillon and K. Chakrabarty, “Sensor placementfor effective coverage and surveillance in distributed sensor networks ” in IEEE Wireless Communications and Networking Conference, 2003, pp.1609–1614.
3. G. Cao, G. Kesidis, T. L. Porta, B. Yao, and S. Phoha, “Purposeful mobility in tactical sensor networks” Sensor Network Ope rations, 2006.
4. S.A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, J. Ma,”Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing” In International Conference on Advanced Information Networking and Applications Workshops, vol. 2, pp. 113–120 , 2007.
5. I. Amundson, X. Koutsoukos, J. Sallai,” Mobile sens or localization and navigation using

RF doppler shifts” In 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments, MELT 2008.

Приходько Владислав Олександрович
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ОБЪЕКТОВ. ВЫБОР ЭФФЕКТИВНОГО РЕШЕНИЯ

Основное назначение СКУД в системах безопасности - защита от несанкционированного проникновения на охраняемый объект. При решении этой задачи в целом необходим комплексный подход и учет взаимодействия как собственных технических средств СКУД, так и их взаимодействия с другими техническими средствами защиты в составе интегрированной системы безопасности (ИСБ). Рациональное использование всех технических средств, а также правильное организационное построение структуры СКУД и всей ИСБ могут обеспечить высокую эффективность и надежность защиты объекта от несанкционированных проникновений.

Идентификация и аутентификация.

Идентификация - основа работы СКУД. С практической точки зрения процесс идентификации рассматривается как сравнение введенного в систему идентификационного признака (кода) с образцами кодов, хранящимися в памяти системы (поиск и сравнение "одного" со "многими").

Выбор методов и средств идентификации при построении СКУД для защиты различных объектов во многом определяет эффективность защиты от несанкционированного проникновения на охраняемый объект.

Аутентификация - процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта. С практической точки зрения процесс аутентификации рассматривается как сравнение "одного" с "одним".

Идентификация и аутентификация в СКУД могут производиться по следующим основным принципам.

Идентификация по запоминаемому коду - осуществляется по коду (паролю), который должен запомнить человек (пользователь) и который вводится вручную с помощью клавиатуры, кодовых переключателей или

других подобных устройств. Положительной стороной этого метода является то, что нет материального носителя кода и соответственно не требуются затраты на его использование. Однако запоминание кода или пароля человеком имеет определенные недостатки. Зачастую код записывают на бумаге и хранят ее в доступном для потенциального нарушителя месте. При этом секретность доступа практически теряется. Существует еще одна проблема, связанная с проходными на крупных предприятиях. При большом потоке людей ошибки, связанные с неправильным набором кода, резко снижают пропускную способность и порождают множество конфликтов со службой охраны. Клавиатурные считыватели недостаточно защищены от манипуляций (подбор кода, наблюдение). Однако они имеют определенные достоинства: например, разрядность кода может быть выбрана произвольно, код может устанавливаться самим пользователем и произвольно им изменяться и быть неизвестным оператору системы (при соответствующем построении программного обеспечения СКУД). Также имеется возможность ввода дополнительных кодов, например кода "тихой" тревоги при нападении, кодов управления. В настоящее время идентификация по запоминаемому коду применяется в простых автономных устройствах доступа или в качестве дополнительного уровня в СКУД с многоуровневой идентификацией.

Идентификация по вещественному коду выполняется по коду, записанному на физическом носителе (идентификаторе), в качестве которого применяются различные электронные ключи, пластиковые карты, брелоки и т.д. Данный принцип получил в настоящее время наибольшее распространение.

Достоинства и недостатки идентификаторов.

Технология кодирования пластиковых карт и электронных ключей отличается большим разнообразием - от простых и дешевых карт со штриховым кодом до карт с электронной начинкой, по сложности не уступающей ЭВМ. Постоянно появляются новые типы идентификаторов, использующие различные технологии с целью повышения надежности, секретности кода и улучшения других характеристик. Основное качество вещественных идентификаторов с точки зрения их применения в системах безопасности - это защищенность от подделки, копирования и имитации. Перспективной технологией можно считать радиочастотную идентификацию (RFID).

Запоминаемые и вещественные идентификаторы относятся к классу присвоенных идентификационных признаков. Это означает, что идентифицируется не сам человек, а присвоенный ему признак. Отсюда следует основной и весьма существенный недостаток подобных систем - код (пароль) может быть забыт, потерян, подсмотрен посторонним лицом, а идентификатор (предмет) потерян, украден, скопирован или преднамеренно передан постороннему лицу.

Принципиальной защиты от подобных случаев и преднамеренных действий в СКУД с использованием идентификации по запоминаемому и вещественному признаку нет.

Повысить эффективность СКУД в этом случае можно с помощью многоуровневой идентификации. Например, двухуровневая идентификация предполагает использование кодовой клавиатуры и Proximity-карты.

Принципиально задачу защиты от несанкционированного доступа такая идентификация не решает, однако затрудняет работу нарушителей, ведь им в данном случае необходимо украсть или сымитировать карту и узнать код (пароль). Можно также привлечь охранника и выводить на экран монитора фотографию пользователя в момент прохода через турникет, но этот метод фактически означает отказ от автоматизации контроля доступа, что существенно повышает затраты и к тому же усугубляет влияние человеческого фактора.

Биометрическая идентификация.

Кардинальным решением задачи повышения защиты объекта от несанкционированного доступа с помощью СКУД является использование биометрической идентификации, которая более эффективна, так как опознание производится не по присвоенным человеку идентификационным признакам, а по физиологическим свойствам или особенностям самого человека - уникальной персональной информации, которую не нужно держать в памяти, невозможно потерять и имитация которой крайне затруднительна.

Однако основное отличие биометрического способа идентификации от других состоит в том, что решения принимаются системой на основе вероятностного характера полученной информации. В этом случае ошибки в принятии решений неизбежны, и можно говорить только о снижении вероятности появления ошибок. Уровень этих ошибок будет являться критерием качества системы и должен быть указан в руководстве по эксплуатации или, по крайней мере, известен пользователю системы на основании эмпирических данных.

Этот критерий определяется двумя техническими характеристиками:

- вероятностью несанкционированного допуска (ошибка первого рода) - выраженное в процентах число допусков системой неавторизованных лиц;
- вероятностью ложного задержания (ошибка второго рода) - выраженное в процентах число отказов в допуске системой авторизованных лиц.
-

Снижение вероятности ошибок.

Применение биометрических систем связано с некоторыми трудностями и особенностями. Как правило, вероятностные характеристики биометрических считывателей, в которых заложены встроенные алгоритмы распознавания,

указываются и определяются при условии проведения аутентификации, то есть при сравнении "один к одному". При использовании таких устройств в составе больших систем (при числе пользователей порядка сотен и более человек) необходимо переходить от процедуры аутентификации к процессу идентификации. При этом вероятность ошибки первого рода, которая определяет защищенность системы от несанкционированного допуска, существенно снижается.

В такой ситуации на помощь может прийти многоуровневая идентификация, предполагающая использование наряду с биометрическим считывателем клавиатуры или Proximity-карты. В этом случае задача применения дополнительного уровня идентификации заключается в замене процесса идентификации по биометрическим данным аутентификацией, что обеспечивает заданную высокую надежность распознавания и существенно снижает время анализа, так как происходит только сравнение с заданным биометрическим шаблоном. Тем самым достигаются следующие результаты:

- в более полной мере реализуются преимущества биометрических систем в обеспечении защиты объекта от несанкционированного доступа;
- значительно снижаются ограничения по количеству пользователей в биометрических СКУД;
- увеличивается пропускная способность биометрических систем.

Вопрос выбора системы.

При выборе подсистемы контроля доступа в составе системы безопасности нужно учитывать общие принципы построения системы противокриминальной защиты, о которых было сказано выше. Процесс создания системы противокриминальной защиты помимо определения необходимых требований к СКУД включает в себя следующие этапы:

- классификация объекта;
- определение класса защиты объекта от криминальных угроз;
- реализация комплекса организационно-технических мероприятий по приведению системы противокриминальной защиты объекта в соответствие с классом объекта и соответствующим ему классом защиты объекта.

В процессе проектирования должны быть определены классы защиты объекта в целом и отдельных зон и помещений, выбраны технические средства СКУД, обеспечивающие защиту должного уровня.

Определенные трудности в решении этой задачи связаны с тем, что в настоящее время нет единой классификации средств и систем СКУД по уровню защиты охраняемого объекта от несанкционированного проникновения. Создание такой классификации весьма актуально, так как она позволит обоснованно выбирать технико-экономические показатели СКУД.

Работы в этом направлении ведутся многими организациями. Следует отметить, что такая классификация не может быть рассчитана на длительное

время, так как появляются и новые средства защиты, и новые средства ее преодоления. Совсем недавно электронные ключи Touch Memory считались достаточно защищенными от подделки, а сейчас можно заказать их копию на любом рынке, причем это будет проще и быстрее, чем создать дубликат обычного механического ключа. Данный пример лишний раз демонстрирует необходимость актуализации состояния такой классификации, с этой целью работа над ней должна проводиться постоянно.

При выборе технических средств СКУД, метода идентификации (в том числе многоуровневой) следует исходить из принципа равнопрочности средств защиты от несанкционированного проникновения (то есть класс защиты идентификатора от подделки должен соответствовать классу защиты дверей от взлома и замка - от вскрытия и т.д.). Необходимо также учитывать и другие возможности технологий, исходя из задач защиты объекта, степеней угроз и экономических факторов.

Правильное организационное построение структуры СКУД, учет взаимодействия технических средств в составе ИСБ, а также их рациональное использование могут обеспечить высокую эффективность и надежность защиты объекта от несанкционированных проникновений. При этом надо иметь в виду, что выбор сложных (широко рекламируемых и соответственно дорогих) решений может оказаться неэффективным.

Література:

1. G. Cao, G. Kesidis, T. L. Porta, B. Yao, and S. Phoha, “Purposeful mobility in tactical sensor networks” Sensor Network Ope rations, 2006.
2. S.A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, J. Ma,”Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing” In International Conference on Advanced Information Networking and Applications Workshops, vol. 2, pp. 113–120 , 2007.
3. I. Amundson, X. Koutsoukos, J. Sallai,” Mobile sens or localization and navigation using RF doppler shifts” In 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments, MELT 2008.

Кравченко Родион Николаевич
Государственный Университет Телекоммуникаций
Учебно-научный институт Менеджмента и предпринимательства
г. Киев

УПРАВЛЕНИЕ КОНКУРЕНТОСПОСОБНОСТЬЮ ОПЕРАТОРА ТЕЛЕКОММУНИКАЦИЙ

Международный опыт позволяет утверждать, что одним из основных факторов, который будет влиять на развитие национальной экономики,построение в Украина информационного общества, на процесс интеграции Украины в ЕС и в мировую экономику, является ускоренное развитие телекоммуникаций. Увеличение участников телекоммуникационного

рынка привело к обострению конкуренции, которое приводит к тому, что операторы телекоммуникаций стараются не только быть адекватными рыночной ситуации, в частности, предоставляя услуги необходимого для потребителей уровня качества, но и выбирают путь постоянного повышение своей конкурентоспособности, направленного как на сохранение существующих, так и на создание новых конкурентных преимуществ.

Операторы телекоммуникаций постепенно превращаются в новый тип корпораций, имеют следующие характерные черты:

- новая корпорация является креативной. Это означает, что вся ее деятельность призвана создавать новации в различных сферах жизни человека. В каких именно сферах корпорация будет вести деловую активность, зависит от того, какими компетенциями он говорит;
- единственным источником воспроизводства корпорации как органической системы является компетенции, носителями которых, главным образом, выступают высококвалифицированные специалисты;
- основой современных корпораций является соединение знаний в отличие от корпораций в условиях индустриальной системы, основанные на соединении капиталов;
- создаются отношения партнерства между участниками определенной корпорации.

Функционирование национальных телекоммуникационных рынков подчиняется общемировым тенденциям, среди которых можно выделить следующие:

- усиление процесса либерализации и обострения международной конкуренции;
- углубление интеграционных процессов;
- научно-технические и технологические изменения;
- развитие новых методов неценовой конкурентной борьбы и выход
- на инновационный путь развития.

Развитие новых методов конкурентной борьбы и выход на инновационный путь розвитку. В свою очередь, это становится возможным при следующих условиях, когда:

- достигнут высокий уровень проникновения телекоммуникаций;
- построены основные элементы телекоммуникационной сети;
- создана благоприятная среда для конкуренции и инновационного развития со стороны регуляторных органов;
- конкуренция между участниками телекоммуникационного рынка является прозрачной;
- операторы телекоммуникаций выбирают инновационный путь развития в долгосрочной перспективе подобное.

Однако,особенности телекоммуникаций,как сферы,эксплуатирующей средства связи и организует технологический процесс по передаче разнообразной информации, обусловливают существенные различия процессов обеспечения конкурентоспособности телекоммуникационных операторов.

Это касается состава факторов и критериев, влияющих на уровень конкурентоспособности операторов телекоммуникаций, определение и обоснование системы конкурентных стратегий оператора телекоммуникаций разработки и реализации программ повышения конкурентоспособности операторов телекоммуникаций тому подобное.

Литература:

1. Хамел Г. Конкурируя за будущее. Создание рынков завтрашнего дня / Г. Хамел, К. К. Прахалад; пер. с англ. - М .: ЗАО «Олимп-Бизнес», 2002. - 288 с.
2. Прахалад К.К., Рамасвамы В. Будущее конкуренции. Создание уникальной ценности вместе с потребителями / К.К. Прахалад, В. Рамасвамы; пер. с англ. - М .: ЗАО «Олимп-Бизнес», 2006. - 352 с.
3. Тарнавская Н. Новейшие проявления конкуренции в обществе, базируется на знаниях / Н. Тарнавская // Экономика Украины. - № 2. - 2008. - С 4 - 16.
4. Гранатуров В.М., Кораблинова И.А. конкурентоспособность телекоммуникационных компаний: проблемы теории и практики управления. Монография / В.Н. Гранатуров, И.А. Кораблинова. - Киев: Кафедра 2012. - 320 с.
5. World Investment Report 2002: Promoting Linkages // UNCTAD. - Washington, 2002. - 85 p.

Щетініна Анастасія Артурівна
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

SPECIFIC ABSORPTION RATES (SAR)

SAR - удельный коэффициент поглощения (англ. Specific Absorption Rates). Данная величина определяет энергию электромагнитного поля, которая выделяется в тканях человека за одну секунду. SAR измеряется в ваттах на килограмм. С помощью этой величины и определяют уровень излучения мобильных телефонов.

Следует учитывать, что уровень SAR измеряется на максимальной мощности работы телефона. А уровень мощности передатчика изменяется в довольно большом диапазоне и зависит от конкретных условий. Статья о вредном воздействии излучений от мобильного телефона уже публиковалась на форуме ранее. Добавлю только некоторые рекомендации по снижению уровня облучения при использовании сотового телефона:

Для того, чтоб как-то оценивать величину излучения сотового аппарата на организм человека, был придуман показатель «Удельный коэффициент поглощения электромагнитной энергии» — SAR.
SAR является мерой скорости, с которой энергия ВЧ излучения поглощается тканями организма, измеряется в Вт/кг.

Стоит отметить, что величины SAR указываемые в инструкциях для сотовых телефонов, подразумевают работу передатчика на полную мощность, к примеру когда вы находитесь в зоне не уверенного приема.

Для того, чтобы мобильный телефон был сертифицирован величина его SAR не должна превышать определенные нормы. Федеральной комиссией по связи в США (FCC), министерством промышленности Канады (IC), а также регулирующими органами некоторых других стран принята норма SAR равная 1,6 Вт/кг при пересчете на 1 г тканей тела. В странах Европейского Союза принята норма SAR равная 2 Вт/кг для 10 г тканей.

Безопасность сотовых телефонов, по современным представлениям, определяется величиной SAR (удельная поглощенная мощность, выраженная на единицу массы тела или ткани). SAR — это единственный показатель, который принят в мире, как разрешительная санитарная норма для использования мобильников. Но, несмотря на это, в мире не существует единой методики измерения SAR. Опыты проводятся в различных независимых лабораториях и их результаты часто в разы отличаются.

Література:

1. https://www.scienceforum.ru/2016/1531/22761
2. http://1234g.ru/3g/umts/vliyanie-mobilnykh-telefonov-na-zdorove-cheloveka
3. http://sar-mobile.blogspot.com/

Школьный Иван Александрович

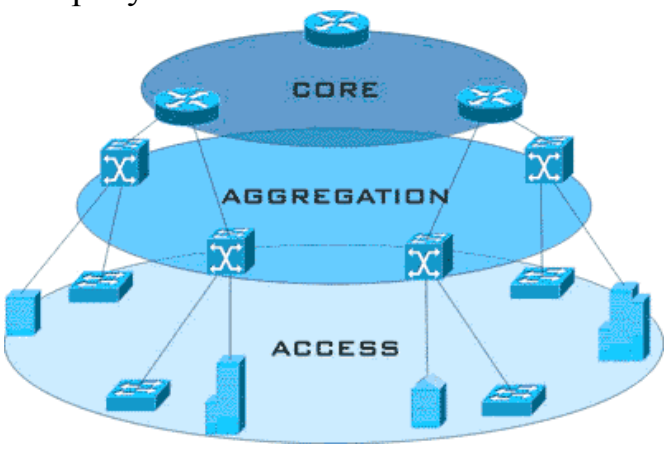
Государственный университет телекоммуникаций

Факультет Телекоммуникаций

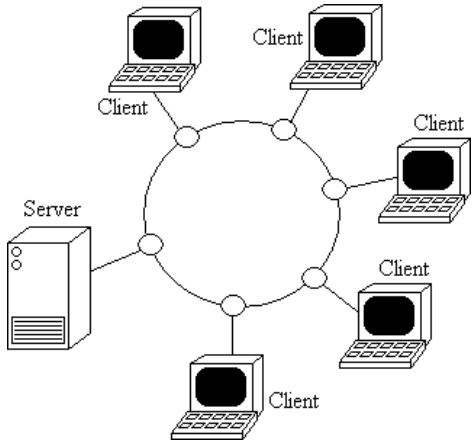
г. Киев

ИСПОЛЬЗОВАНИЕ WDM ПРИ ПОСТРОЕНИИ ГОРОДСКИХ СЕТЕЙ

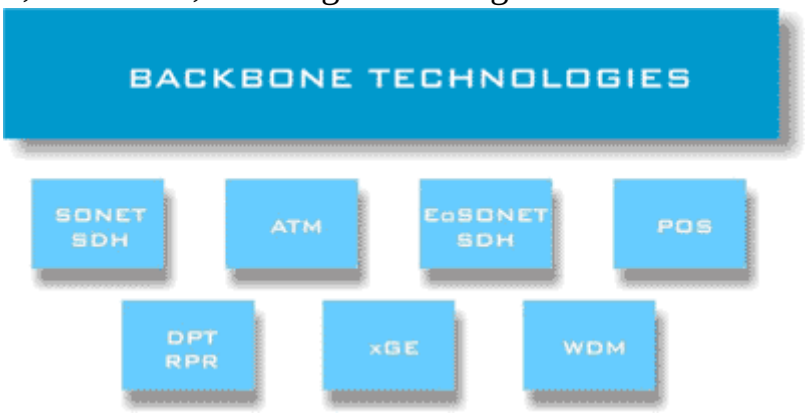
Классическим на сегодня подходом к построению городских сетей является функциональная декомпозиция на уровни доступа: опорная сеть (магистраль), уровень распределения/агрегации, уровень доступа (клиентский доступ), как указано на рисунке:



Для обеспечения повышенной надежности и резервирования широко применяется топологическая модель кольца. Кольца обычно создают на уровнях опорной сети и доступа. На рисунке указана схема построения данной топологии :



Базовыми магистральными технологиями на сегодня являются следующие: SONET/SDH, ATM, POS (Pocket over Sonet), EoSDH (Ethernet over SDH), DWDM, CWDM, DPT/RPR, Fast/Gigabit/10 Gigabit Ethernet etc.



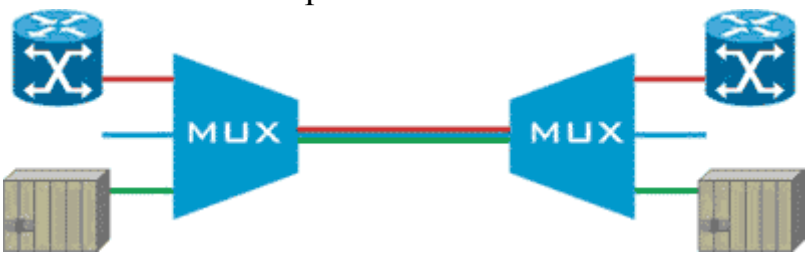
Кратко рассмотрим некоторые из указанных технологий:

ATM

В свое время с целью создания мультисервисной (для всех существовавших видов трафика: голос, видео, интернет) и высокоскоростной технологии передачи данных появилась Asynchronous Transfer Mode – ATM. Повсеместного распространения (несмотря на известный лозунг "ATM everywhere") не получилось (в локальных сетях победил Ethernet), но для построения магистралей ATM стала базовой на многие годы. Ориентация на высокие скорости определила наиболее предпочтительную физическую среду передачи для ATM – оптическое волокно. Очень часто магистральные сети ATM выполняются наложением на существующую инфраструктуру SONET/SDH, что изначально предусмотрено стандартом . Однако данный метод неэффективен и, естественно, уступает непосредственному соединению ATM-оборудования.

Ethernet (FE,GE, xGE)

Технология Ethernet в своем стремительном развитии уже давно перешагнула уровень локальных сетей. Она избавилась от коллизий, получила полный дуплекс и гигабитные скорости.

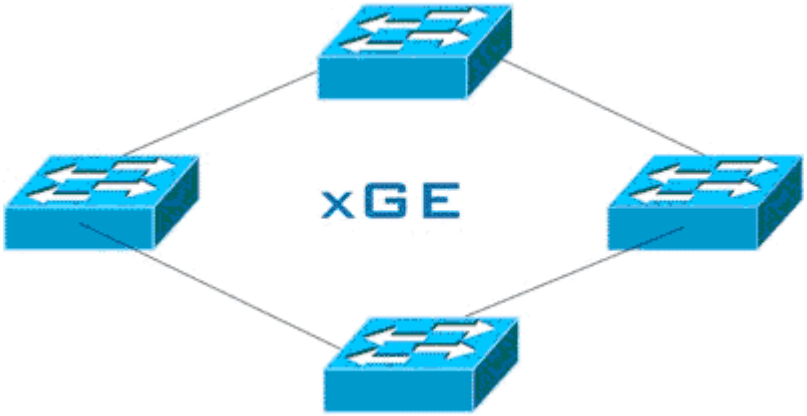


В настоящее время отмечается подавляющее преобладание IP-трафика в потребительских сетях. И вот уже для передачи TDM-сигналов (например, для связи между цифровыми АТС) разрабатывается протокол TDMoIP, эмулирующий TDM-каналы, прозрачные для всех протоколов и сигнализаций. Если раньше пакеты транспортировались в сетях с коммутированием каналов, то теперь все может измениться с точностью до наоборот.

Базовые контрольно-управляющие технологии

VLAN

Без сомнения, базовой для построения развитых Ethernet-сетей является технология виртуальных локальных сетей – Virtual LAN (VLAN). Она позволяет создавать в едином Ethernet-сегменте независимые логические области, ограничивающие на канальном уровне пределы распространения трафика (в том числе и широковещательного). Для этого (согласно стандарту IEEE 802.1Q) в заголовок Ethernet-фрейма вводится дополнительная информация о принадлежности к вилану (VLAN). Так получается вилан с помеченными кадрами данных (Tagged VLAN), которые передаются по транковым линиям (802.1Q Trunk). Это позволяет передавать по одному каналу данные нескольких изолированных локальных сетей. Дальнейшая коммутация происходит с учетом 802.1Q-метки. На выходе из коммутатора (например, на стороне клиентского порта) метка (Tag) убирается (это называется вхождением порта в нетегированный вилан – Untagged VLAN).



Хрестоматийный дизайн сети под названием "эскимо" ("маршрутизатор на палочке" – "router on stick") выглядит следующим образом: клиентские

подсети изолируются друг от друга путем подключения к раздельным виланам (через порты с Untagged VLAN), а связь между ними организуется при помощи маршрутизатора (Layer 3 OSI) через 802.1Q транки (содержащие Tagged VLAN)

STP

Как известно, в сетях Ethernet коммутаторы поддерживают только древовидные, то есть не содержащие петель связи. И именно технология Spanning Tree Protocol (STP) позволяет создавать отказоустойчивые топологии канального уровня (Layer 2 OSI) типа "кольцо", являясь совершенно прозрачной для вышестоящего стека сетевых протоколов (IP).

Принцип действия STP выглядит следующим образом. После активирования коммутаторы обмениваются специальными информационными пакетами (BPDU) с помощью которых вначале выбирается корневой мост (который будет в итоге находиться на вершине древовидной структуры) а затем кратчайшие (в смысле пропускной способности) пути от каждого из коммутаторов до корневого. В конечном итоге формируется логическая беспетельная топология путем блокирования некоторых избыточных связей (портов).

В настоящее время все большее признание получает Rapid Spanning Tree Protocol (RSTP) – учитывающий ограничения и недостатки STP стандарт.

Рассмотрим роль WDM в построении сетей масштаба города.

Непрерывно возрастающие объемы трафика требуют повышения пропускной способности оптических магистралей. Кроме тривиального повышения скоростей передачи существует и другой способ решения данной задачи – уплотнение (мультиплексирование) каналов. Наиболее развитой в настоящее время является технология оптического спектрального уплотнения, называемая обычно мультиплексированием с разделением по длине волны – Wavelength Division Multiplexing (WDM).

Исторически первыми возникли двухволновые системы WDM, работающие на центральных длинах волн из второго и третьего окон прозрачности кварцевого волокна(1310 и 1550 нм). Главным достоинством таких систем является то, что из-за большого спектрального разноса полностью отсутствует влияние каналов друг на друга. Этот способ позволяет либо удвоить скорость передачи по одному оптическому волокну, либо организовать дуплексную связь.

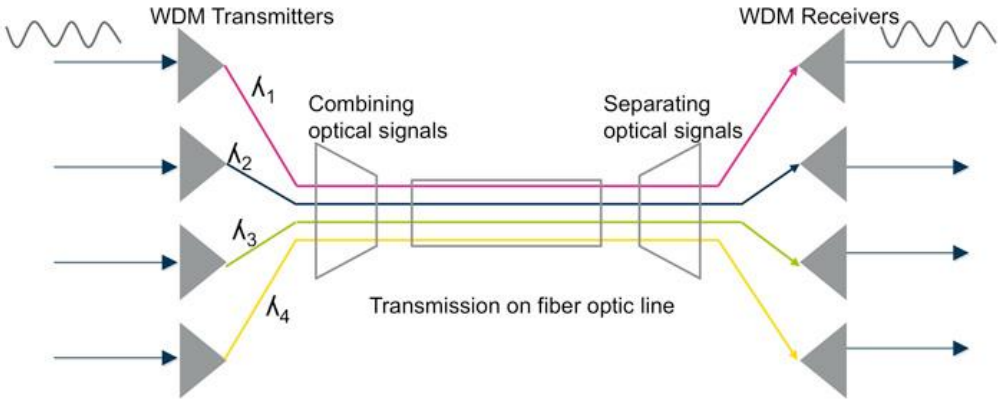
Современные системы WDM на основе стандартного частотного плана (рекомендация G.692 ITU-T) можно подразделить на три группы:

- грубые WDM (англ. coarse WDM, сокр. CWDM) — системы с частотным разносом каналов более 2500ГГц, позволяющие мультиплексировать не более 18 каналов. Используемые в настоящее время CWDM работают в

полосе от 1271нм до 1611нм, промежуток между каналами 20нм (2500 ГГц), можно мультиплексировать 16 спектральных каналов;

- плотные WDM (англ. dense WDM, сокр. DWDM) — системы с разносом каналов около 100 ГГц, позволяющие мультиплексировать до 40 каналов;
- высокоплотные WDM (англ. high dense WDM, сокр. HDWDM) — системы с разносом каналов 50 ГГц и менее, позволяющие мультиплексировать более 64 каналов.

Принцип действия технологии очень прост: потоки данных от отдельных источников переносятся световыми волнами разной длины (каждому каналу принадлежит своя длина) и объединяются мультиплексором в единый многочастотный сигнал, который передается по оптическому волокну. На приемной стороне происходит обратное преобразование.



Данные одновременно передаются по двум кольцам в противоположных направлениях (тем самым эффективно используя пропускную способность). Поток данных в каждом кольце включает непосредственно транспортируемые в данном кольце данные и контрольные пакеты для соседнего кольца.

В итоге, стандарт 802.17 (вобравший в себя DPT/RPR) позиционируется как высокоскоростная технология динамической передачи IP-пакетов, предназначенная для решения задач построения нового поколения сетей Metro. Для данной технологии физическая оптическая среда совершенно прозрачна (это может быть SONET/SDH, WDM, Ethernet, Dark Fiber).

Налицо преимущества:

- данный протокол отвечает современным требованиям – он пакетно-ориентирован;
- не требуется дополнительная прослойка типа ATM для доступа к физической оптической среде;
- заложен высокий уровень резервирования (все-таки кольца) и быстрая восстановимость в случае аварий (50 мс);
- очень эффективно используется емкость оптических каналов за счет смешения контрольных и передаваемых данных;

- потребители наконец-то поняли, почему им нужен MPLS. Ведь интерфейсы оборудования в кольцах 802.17 получают IP-адреса и все, что с этим связано.

А если требуется QoS, Traffic Engeneering, VPN или просто Layer 2 сервисы (например Ethernet соединения), то в данном случае без MPLS не обойтись.

Можно сделать вывод:

Технология WDM позволяет существенно увеличить пропускную способность канала (к 2003 году, в коммерческих системах достигнута скорость 10,72 Тбит/с, а к 2015 — 27 Тбит/с), причем она позволяет использовать уже проложенные волоконно-оптические линии. Благодаря WDM удается организовать двустороннюю многоканальную передачу трафика по одному волокну. Преимуществом DWDM-систем является возможность передачи высокоскоростного сигнала на сверхдальние расстояния без использования промежуточных пунктов (без регенерации сигнала и промежуточных усилителей). Эти преимущества крайне востребованы на сегодня, поскольку потребности клиентов с каждым днем возрастают.

Pokhabova Iryna
Post-graduate student
State university of telecommunications
Kyiv

FRAMEWORK OF SOFTWARE-DEFINED NETWORKING

SDN is a set of techniques that enables users to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

Figure 7-1 depicts the basic concept of SDN

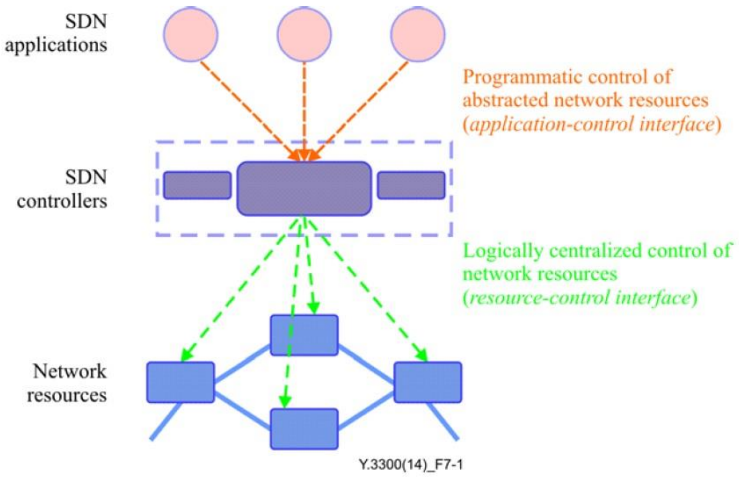


Figure 7-1 – Concept of SDN

SDN relocates the control of network resources to a dedicated network element, namely SDN controller, which provides a means to program, orchestrate, control and manage the network resources through software (i.e., SDN applications).

The distributed network resources perform the network functions such as data packet transport and processing, but the behaviors of network resources are directly controlled via a standardized interface (i.e., *resource-control interface*) and the relevant information and data models.

The SDN controller uses the interface and arbitrates the control of network resources in a logically centralized manner.

The SDN controller manages and configures the distributed network resources and provides an abstracted view of the network resources to the SDN applications via another standardized interface (i.e., *application-control interface*) and the relevant information and data models. The SDN application can customize and automate the operations (including management) of the abstracted network resources in a programmable manner via this interface. Note that the SDN controller can provide different types of interfaces to SDN applications (e.g., more abstracted and more object-oriented).

The objectives of SDN are to realize:

– *Faster network business cycles*

SDN reduces the response time of business requests to network providers, e.g., to increase customer satisfaction or to shorten the payback time of investment through further automation of network operations;

– *Acceleration of innovation*

SDN accelerates business and/or technical innovation through more flexibility of the network operations, thus making trials easier;

– *Accelerated adaptation to customer demands*

SDN facilitates the accommodation of customer's connectivity requirements by means of dynamic negotiation of network service characteristics and of dynamic network resource control;

– *Improved resource availability and usage efficiency*

SDN is meant to improve network resource availability and efficiency, in particular when combined with network virtualization, due to the introduction of a high level of automation in the overall service delivery and operation procedures, from service parameter negotiation to fulfilment and assurance;

– *Customization of network resources including service-aware networking*

SDN allows network customization for the network services which have different requirements, through the programming of network resource operations, including the dynamic enforcement of a set of policies (e.g., resource planning as a function of the number of customers' orders to be processed over time, forwarding and routing, quality of service (QoS) and traffic engineering, security).

High-level capabilities

SDN provides the following high-level capabilities:

– *Programmability*

The behaviour of network resources can be customized by SDN applications through a standardized programming interface for network control and management functionality. The user of the interface may be network providers, service providers, and customers including end-users. This enables the SDN applications to automate the operations of network resources according to their needs.

– *Resource abstraction*

The property and behaviour of underlying network resources can be appropriately abstracted and understood, orchestrated, controlled and/or managed by those who program them, thanks to relevant, standard information and data models. These models provide a detailed, abstracted view of physical or virtualized network resources. Programmability contributes to the introduction of a high level of automation in the overall service delivery procedure, to achieve business agility, such as dynamic service creation and provisioning. A standardized interface providing a channel for interactions between SDN applications and SDN controllers is used to access network information and to program application-specific network behaviors. This programmability provides the ability to control or configure the network elements by a logically centralized SDN controller through another standardized interface.

Requirements

SDN provides programmability of network control and abstraction of underlying network resources, among other SDN features. As described in clause 6, network resources as used in this context of requirements refer to network elements including switches and routers.

In order to support these capabilities, the requirements for SDN are described as follows:

– SDN is required to support programmability of network resources;

– SDN is required to support orchestration of network resources and SDN applications;

– SDN is required to provide an application-control interface for customizing the behavior of network resources;

– SDN is required to provide a resource-control interface for control of network resources;

– SDN is required to provide logically centralized control of network resources;

– SDN is required to separate SDN control from the network resources;

– SDN is required to support the abstraction of underlying network resources, by means of standard information and data models;

– SDN is required to support the management of physical network resources;

– SDN is recommended to support the management of virtual network resources.

High-level architecture

The high-level architecture of SDN consists of several layers as depicted in Figure 11-1.

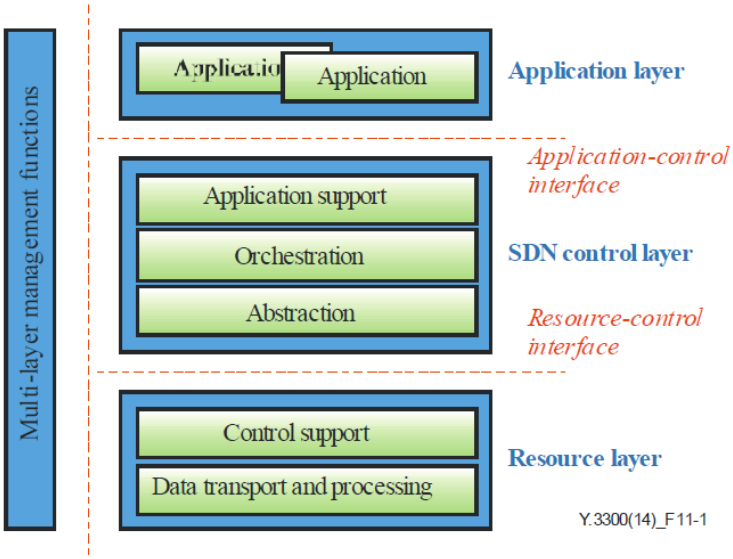


Figure 11-1 – High-level architecture of SDN

Application layer

The application layer is where SDN applications specify network services or business applications by defining a service-aware behaviour of network resources in a programmatic manner. These applications interact with the SDN control layer via application-control interfaces, in order for the SDN control layer to automatically customize the behaviour and the properties of network resources. The programming of an SDN application makes use of the abstracted view of the network resources provided by the SDN control layer by means of information and data models exposed via the application-control interface.

SDN control layer

The SDN control layer provides a means to dynamically and deterministically control the behavior of network resources (such as data transport and processing), as instructed by the application layer. The SDN applications specify how network resources should be controlled and allocated, by interacting with the SDN control layer via application-control interfaces. The control signaling from the SDN control layer to the network resources is then delivered via resource-control interfaces. The configuration and/or properties exposed to SDN applications are abstracted by means of information and data models. The level of abstraction varies according to the applications and the nature of the services to be delivered.

– *Application support*

The application-support function provides application-control interface for SDN applications to access network information and program application-specific network behaviours.

– *Orchestration*

The orchestration function provides the automated control and management of network resources and coordination of requests from the application layer for network resources based on the policy provided by the multi-layer management

functions or the application layer. The orchestration function provides control and management of network resources covering management of physical and virtual network topologies, network elements, and traffic for example. It also interacts with the multi-layer management functions to provide management of SDN application related operations such as user management, service creation and provisioning.

– *Abstraction*

The abstraction function interacts with network resources, and provides an abstraction of the network resources, including network capabilities and characteristics, in order to support management and orchestration of physical and virtual network resources. Such abstraction relies upon standard information and data models and is independent of the underlying transport infrastructure.

Resource layer

The resource layer is where the network elements perform the transport and the processing of data packets according to the decisions made by the SDN control layer, and which have been forwarded to the resource layer via a resource-control interface.

– *Control support*

The control support function interacts with the SDN control layer and supports programmability via resource-control interfaces.

– *Data transport and processing*

The data transport and processing function provides data forwarding and data routing functionalities. The data forwarding functionality handles the incoming data flows to forward them along the data forwarding paths that have been computed and established according to the requirements defined by the SDN applications. The control of the data forwarding functionality is provided by the SDN control layer so that the data forwarding functionality in the resource layer may be minimized. The data routing functionality provides network control and services in the resource layer according to the routing rules which can be customized by the SDN control layer for SDN applications. The data forwarding paths are determined by distributed routing control of the resource layer. The resource layer may provide either data forwarding functionality or data routing functionality, or both. Additional functionalities including media transcoding and data compression can be added, removed, or reconfigured for customization of data packets as specified by SDN applications.

Multi-layer management functions

The multi-layer management functions exist as cross-layer functions providing functionalities for managing, as appropriate, the functionalities of the other layers, i.e., the application layer, the SDN control layer and the resource layer. The multi-layer management functions include functionalities for supporting fault, configuration, accounting, performance and security (FCAPS) management as described in [ITU-T M.3400]. Examples of such functionalities are equipment inventory, software upgrade, fault isolation, performance optimization, energy efficient operations, and initial configuration of the network resources, SDN controllers, and SDN applications. Specifically, autonomic management, i.e.,

continuous adaptation to the network status, may be performed by the SDN control layer.

Interfaces

There are two interfaces in the high-level architecture of SDN: the application-control interface and the resource-control interface. They provide access to the SDN controllers and network resources, allowing for programmable control of network resources.

The details of each interface are as follows:

– *Resource-control interface*

The resource-control interface is used for interactions between the SDN control layer and the resource layer. Information exchanged through these interactions include controlling information provided by the SDN control layer to the resource layer (e.g., for configuring a network resource or providing policies) as well as the information that pertains to the (unsolicited) notifications sent by the resource layer whenever the network topology changes, congestion is detected, etc. Such notification information also includes data that are meant to assess the conformance of what has been delivered against what has been negotiated (hence the notion of service fulfillment and assurance). This interface provides high-level accesses to the network resources regardless of their respective technology.

– *Application-control interface*

The application-control interface is used for interactions between the application layer and the SDN control layer. The application-control interface can be used by the application layer to feed the SDN control layer information that will contribute to the decision-making process in terms of dynamic resource allocation or policy enforcement, for example. The SDN control layer can also expose the information and data models that reflect the resource abstraction to the application layer through this interface.

Environmental considerations

SDN is meant to facilitate self-adaptability, so that resource availability and usage efficiency can be improved. This is likely to contribute to the optimization of resource usage and therefore reduced energy consumption. SDN relocates the control of network resources to a logically centralized SDN controller. This may contribute to simplify the design of network elements, thus power consumption is expected to decrease. However, the function that is logically centralized may become complicated, thus its power consumption may increase.

Security considerations

The introduction of a high level of automation in the overall service delivery procedure by means of SDN techniques inevitably raises security challenges. In particular, access to network resources by applications must be granted in order to protect the networking infrastructure and its components from a denial of service attack that may jeopardize the overall robustness, quality and reliability of the SDN architecture, or the services that it delivers. SDN provides new possibilities to combat security breaches. The affected resources may be easily and quickly isolated,

malicious traffic may be safely terminated, sensitive flows can be identified and separately transferred in a more secure manner, e.g., with dedicated equipment and security protocols. All these processes may be automated due to SDN for improved availability. Moreover, a logically centralized control of SDN enables operators and/or entities to have a broader and/or a global view of the current status of networks, which makes security operations easier and more efficient. On the other hand, SDN may aggravate the damage of security breaches, misconfiguration, privacy infringement and other incidents. Properties that were traditionally implemented in hardware and impossible to change can now be modified, misconfigured or can function improperly. Such damage can expand quickly as responses of various software programs and human operation may be too slow for appropriate reaction. It is therefore necessary to enhance monitoring capability and automated operations. More careful checking of e.g., policy configuration, becomes necessary. Moreover, a logically centralized controller can be a single point of failure, and can be a target of malicious attacks, thus special attention is required.

Areas for further considerations in SDN standardization

Interworking

A network in one administrative domain is usually controlled and managed by the service policy applied by one network provider. However, integrated network services among multiple administrative domains need to be composed of relevant network services in each administrative domain. It is important that SDN provides interworking functionality for such integrated network services among multiple administrative domains taking into account the following points:

– It is important that SDN exchange available network parameters (e.g., bandwidth, latency, label or id information) for automating the control and/or management of the network services among different administrative domains. These network parameters may be screened or abstracted because such network parameters contain sensitive information in many cases. This functionality may also need to configure a part of other administrative domain networks and get statistics about the domain. The following points are not specific to SDN, but need consideration.

– In forwarding packets across multiple administrative domains, packet formats may be different, and it is important to support converting the format of packets and/or adjusting the network properties (e.g., bandwidth and latency) before or after packets enter another network;

– It is also important to support authentication, authorization, and accounting (AAA) features because interworking operations usually need computational resources from other administrative domains.

Verification of SDN applications

With SDN technologies, network providers, service providers, and customers can customize the network resources by writing an SDN application. However, incomplete or malicious SDN applications could cause a breakdown of underlying networks shared by heterogeneous network elements and stakeholders. Thus, it is desirable that SDN applications be formally specified and verified (i.e., formal

method) to prevent them from misinterpreting their intentions on network operations and to avoid inconsistency within the network. Formal methods are software engineering techniques based on mathematical representation and analysis of software programs. Such formal methods can be used for analysis of specification and verification of software behaviour. Using the formal methods for SDN applications can minimize the risk of misuse or malfunction of SDN applications because the formal method serves to remove ambiguity, inconsistency, and possible conflicts of SDN applications in the networks. Furthermore, network operators can use the formal methods to check consistency and safety of their network configurations, virtual/physical topologies and networking resources. This enables confirmation of their configurations and behaviours of various networking properties. Some examples of these properties are:

– no routing loops or unreachable points in the network;

– no rule or behaviour conflicts between multiple SDN applications;

– no conflicts on physical network resource assignments between different SDN applications;

– no conflicts in dynamic network update where new or updated network configurations conform to properties of the network and do not break consistency of existing networks.

Adaptation to large-scale networks

SDN should provide connectivity from a local area to a wide area, as current networks do. Because SDN provides logically centralized control of networks, adaptation to large-scale networks is important. A large-scale network has two aspects: a single SDN domain composed of many network elements, and multiple SDN domains managed by different network providers. While SDN may support many network elements in a wide area, the number of network elements that a single SDN controller can accommodate is limited. In this regard, scalability needs to be considered. One way to provide scalability is to have SDN controllers logically centralized but physically distributed, to correspond to a wide area. In large-scale networks, reliability is a particularly important issue. As a characteristic of logically centralized control in SDN, an SDN controller tends to become a single point of failure. The SDN controller may be replicated to improve reliability.

Design of resource abstraction

To make programmability of SDN easier and more efficient, it is important that resource abstraction is appropriately designed and adopted for the best practice and performance of networks. It is important that resource abstraction be provided with the following points:

– *Common resource abstraction model*

It is important that a common resource abstraction model be applied to similar network resources regardless of the underlying technology, since a common information model simplifies the programming for the resources. Widely applicable standard information and data models require the appropriate abstraction of various

capabilities, such as packet forwarding, wireless interfaces, and path computation-related information (e.g., routing metrics).

– *Appropriate granularity of abstraction*

It is not appropriate to show all network resources and their characteristics to SDN applications. On one hand, not all the details and characteristics of the network resources are necessary for SDN application programming. On the other hand, excessive abstraction prevents SDN applications from utilizing network resources to the maximum because it hides the details of the resources. It is therefore important that SDN provides an appropriate and balanced granularity of abstraction.

– *Performance tuning of network resources*

When network resources are abstracted, an SDN application may not be able to access some network resource-specific parameters, and this may degrade the performance. Suitable abstraction or some mechanisms to tune the performance of network resources automatically are necessary.

Virtualization of network elements

Network elements, which can be abstracted resources, may be shared among multiple applications. But each SDN application does the programming of network elements according to the SDN application requirements. In that case, it is necessary that these networks and network elements are mutually isolated. Toward this end, network elements should be virtually partitioned to support each application network. SDN applications may require network resources, e.g., bandwidth and packet processing, whereas the applications' requirements cannot be satisfied with a single network element. In that case, multiple network elements can be virtually combined to appear as a single resource to the applications to satisfy the requirements without further management efforts of multiple network resources. For the above two cases, virtualization techniques can provide an appropriate solution because they massume network element partition and aggregation, as well as a single interface to such virtualized network resources.

Multiple-level of programmability

In conventional networks, each resource in multiple open system interconnection (OSI) layers [b-ITU-T X.200] is managed by different management entities. This makes it difficult to orchestrate total performance and to recover from network failures quickly. SDN is desirable to provide control and management programming interfaces to network resources, e.g., for coordination and status monitoring purposes. In addition, the demands of SDN applications can be diverse and may be related to multiple OSI layers. The interfaces need to span multiple OSI layers and work in a unified manner: multiple-level of programmability that spans L1-L7 OSI layers is an important issue to be addressed for SDN. One example for such multi-level programmability is cut-through optical path computation. In this example, some SDN components may dynamically change the target OSI layer to allocate a path, depending on traffic characteristics. For example, SDN components may first allocate a path in the OSI layer 3, namely an IP route. After checking OSI layer 3 header and

its applicability, SDN intelligence may then decide instead to allocate an optical path, e.g., to provide additional bandwidth.

Programmatic extension in resource layer

In order to improve network programmability, it is desirable to extend the functions of the resource layer on demand in a programmable manner [b-SDN-WS Nakao]. This ability can dynamically add or remove additional functions for data transport and processing (such as packet caching, header/payload compression, regular expression matching, data transcoding, or even handling newly developed protocols) as per SDN application requirements or can dynamically update the control support function, thereby avoiding hardware replacement. Thus, rapid development, deployment, and replacement of resource layer functionalities and resource-control interfaces leads to timely and tailored service solutions aligned with requirements of applications and operator policies.

Management

The following management functionalities specific to one of the layers need to be further considered:

– Management of the underlying physical and virtual network resources, providing support for programmatically extendable SDN data transport and processing functions;

– Management of the software and hardware platform of an SDN controller which includes lifecycle management of dynamically upgradable functions of the SDN controller and FCAPS. The multi-layer management functions should interoperate with 3rd party management functions, for example, for billing, customer care, statistics collection or dynamic service provisioning. Another issue to be considered is how the multi-layer management functions are deployed. Possible approaches include the use of a centralized management model or a hybrid model. In the hybrid model, some management functions are distributed, while others are implemented in centralized management systems. With such an approach, network resources support management functions that may improve network robustness and scalability as well as shorten the management system response time. In both models, there is an SDN management system that performs all centralized management operations.

Bibliography

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.*

[b-ITU-T Y.2622] Recommendation ITU-T Y.2622 (2012), *Architecture of an independent scalable control plane in future packet based networks*.

[b-ETSI NFV] ETSI NFV ISG, *Network Functions Virtualisation*,
http://portal.etsi.org/portal/server.pt/community/NFV

[b-IETF I2RS] IETF I2RS Working Group, *Interface to the Routing System*,
http://datatracker.ietf.org/wg/i2rs/charter/

[b-IETF RFC 3444] IETF RFC 3444 (2003), *On the Difference between Information Models andData Models*.

[b-IETF RFC 3746] IETF RFC 3746 (2004), *Forwarding and Control Element Separation (ForCES) Framework.*

[b-IETF RFC 7149] IETF RFC 7149 (2014), *Software-Defined Networking: A Perspective from within a Service Provider Environment*.

[b-IETF SFC] IETF Service Function Chaining (sfc) working group, http://datatracker.ietf.org/wg/sfc/charter/

[b-ONF] Open Networking Foundation, "OpenFlow/Software-Defined Networking (SDN)," https://www.opennetworking.org/.

[b-OpenDayLight] Linux Foundation, OpenDayLight, http://www.opendaylight.org/.

[b-SDN-WS Nakao] "*Deeply Programmable Network*", Emerging Technologies for Network Virtualization, and Software Defined Network (SDN), ITU-T Workshop on Software Defined Networking (SDN), http://www.itu.int/en/ITU-T/Workshops-and-Seminars/sdn/201306/Documents/KS-Aki_Nako_rev1.pdf.

[b-FM Clarke] Edmund M. Clarke and Jeannette M. Wing (1996), *Formal methods: State of the art and future directions*, ACM Computing Surveys Vol. 28, No. 4, December; pp. 626-643.

Короленко С.
Державний Університет Телекомунікацій
Випускник ДУТ
Kyiv

КІБЕРВІЙНА. ЛОКАЦІЯ – ІНТЕРНЕТ

Сьогодні вже ніхто не сумнівається у важливості інформаційних технологій в нашому житті. Обчислювальна техніка приймає за рішення за нас, зберігає наші секрети, управляє електростанціями, допомагає робити складні медичні операції. Це зручніше та швидше. Але чим глибше інформаційні технології проникають в наше життя, тим більше буде шкода, які вони можуть завдати в результаті атак кіберзлочинців.

Вересень 2010 - вірус Stuxnet завдав серйозної шкоди іранській ядерній програмі. Використовуючи вразливості операційної системи і людський фактор, Stuxnet вразив 1368 з 5000 центрифуг на заводі зі збагачення урану в Натанзі, а також відклав запуск ядерної АЕС в Бушері. 23 грудня 2015 вже Івано-Франківська область залишилася без електропостачання в результаті атак на "Прикарпаттяобленерго" за допомогою шкідливих програм Black Energy 3 і KillDisk.

Важливість інформаційної безпеки зараз складно переоцінити. 3 світова війна вже почалася, охоплення - планета Земля, локація - інтернет. Для молодих фахівців в сфері ІБ це означає зростання популярності на їх навички і знання.

Доступ до інформації та управління нею - потужний важіль влади, валюта, яку всі країни намагаються контролювати. Для країни важливо, щоб цінний ресурс у вигляді знань і умінь висококваліфікованих фахівців не витікав за кордон. Адже той факт, що 1 фахівець може негативно вплинути на безпеку великої держави лякає. Взлом твіттера каналу BBC з повідомленням "Термінова новина: два вибухи в Білому домі. Барак Обама поранений" привів до падіння котирувань на фондовому ринку і втрати мільярдів доларів. Такі

фахівці мають велику силу і великою відповідальністю. Спроби обмежити, переслідувати чи керувати такими людьми призведе до ворожнечі і посилення атак. Суспільство має розуміти, що нестандартне мислення, підхід до пошуку вразливостей це те, що ми повинні цінувати і намагатися направляти таких фахівців на світлу сторону сили. Замість пригнічення та навязування стереотипу, що хакер – це людина, що прагне збагачення шляхом обкрадання банків та інших людей ми повинні збагнути, що хакери – це сканери вразливостей у сучасному світі. Вони як МРТ – знаходять пухлини в організмі, яким є програмне забезпечення. Шлях, який вони оберуть після знахідки вразливості визначає, до якої сторони сили вони належать.

Поділяють хакерів на BlackHat та WhiteHat. Якщо після знахідки можливості обходу захисту кардіостимулятора, або ж можливості читати переписку у фейсбук спеціаліст повідомить про це розробників – це WhiteHat. До 2010-х за такі знахідки фахівець не отримував жодної винагороди, а інколи навіть відкривалося кримінальне впровадження на основі незаконного втручання в роботу інформаційних систем. На теперішній час існують інтернет платформи такі як bugcrowd та hackerone на яких опубліковано список інтернет-ресурсів та умов, за якими спеціаліст з інформаційної безпеки може отримати винагороду. Кожен може зареєструватися та перевірити свої навички з пошуку вразливостей, описати свої знахідки та отримати грошову винагороду. Це гарний приклад того, як можна використовувати могутність хакерів в мирних цілях.

Література:

1. https://hackerone.com/ платформа, що виплачую винагороду за знайдені вразливості в інформаційних системах.
2. https://bugcrowd.com/ платформа, що виплачую винагороду за знайдені вразливості в інформаційних системах.
3. https://habrahabr.ru/ інформаційний ресурс для IT-специалистов.
4. http://www.bbc.com/russian/rolling_news/2013/04/130423_rn_associated_press_hacked.shtml «Хакеры сообщили о "ранении Обамы" через Twitter AP», 23 квітня 2013 року.

Буртак Артем Володимирович
Національна академія внутрішніх справ
курсант 3-го курсу
м. Київ

«UNIVERSAL INFORMATION SECURITY POLICE PLATFORM»

«УНІВЕРСАЛЬНА ПЛАТФОРМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПОЛІЦІЇ»

У статті проаналізовано проблемні аспекти глобальної інформаційної безпеки. Визначено концепцію, яка може бути покладена в основу розробки інституційно-правових норм, організаційно-технічних заходів, вимог та методів для забезпечення визначення глобальних стандартів інформаційної безпеки поліції. Розглядаються практичні випадки вразливості технологій вірусами, хробаками та шпигунськими програми. Зазначено, яким чином прогресує кіберпростір, розвивається кіберзлочинність та стандарти інформаційної безпеки поліції.

Along with the changing face of conflict, terrorism and crime - cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices. It is gaining relevance because computer now carries out many tasks that were once carried out by hand. Therefore there is a need for information assurance and security [1].

The purpose and objectives. Based on the current state of crime and measures to combat it requires a reconsideration of the question of improving suppression of individual groups of offences: in the field of cyberspace and cybersecurity which in practice requires in implementing individuals approach in the fight against international crimes [2].

Cyber terrorism is typically defined as using the internet as a tool for launching an attack. Terrorism and the Internet are related in two main ways. First, the Internet has become a forum for terrorist groups and individual terrorists both to spread their messages of hate and violence and to communicate with one another and their sympathizers. Secondly, individuals and groups have tried to attack computer networks, including those on the Internet, what has become known as cyber terrorism or cyber warfare. Digital development index is indicator that measures the level of Information Communication Technology (ICT) adoption of countries. Purpose of this article is to find correlation functions of Denial-of-Service (DoS) attacks (most known cyber terrorist method), index of digital development of countries, and provide information of their relations [4].

A 2016 US security framework adoption study reported that 70% of the surveyed organizations see the NIST Cybersecurity Framework as the most popular best practice for computer security, but many note that it requires significant investment [5].

Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies [5].

The Internet and technology have penetrated nearly every aspect of our daily lives. This has created many positive conveniences, but also provides criminals with opportunities to reach new victims [3].

It is important to protect yourself and your devices from criminals who wish to exploit them. However, technology is constantly evolving and criminals are always finding new ways to manipulate it, so you must always remain vigilant and adopt new safety measures on a regular basis [1].

It is also necessary to pay attention for the problem with mobile phones. Nowadays, mobile phones have become ubiquitous and basic communications tools - now used not only for phone calls, but also for accessing the Internet, sending text messages, and documenting the world. Unfortunately, mobile phones were not designed for privacy and security. Not only do they do a poor job of protecting your communications, they also expose you to new kinds of surveillance risks - especially location tracking. Most mobile phones give the user much less control than a personal desktop or laptop computer would; it's harder to replace the operating system , harder to investigate malware attacks, harder to remove or replace undesirable bundled software, and harder to prevent parties like the mobile operator from monitoring how you use the device. What's more, the device maker may declare your device obsolete and stop providing you with software updates, including security fixes; if this happens, you may not have anywhere else to turn for these fixes. Some of these problems can be addressed by using third party privacy software - but some of them cannot [2].

As the largest international law enforcement organization, Interpol is ideally placed to create bridges between the police community and information security professionals worldwide and thereby to co-ordinate the development of global police information security standards [4].

The force recognizes the importance of all information assets and the need for proper, effective management of all information processes. It is essential therefore that there are safeguards and counter measures in place to provide the continued confidentiality, integrity and availability of force information. [6].

Besides providing a platform to exchange good practices and valuable experiences, the conference will be a great opportunity to understand common threats faced by different regions of the world and to forge partnerships in identifying solutions," said Hong Kong's Commissioner of Police [1].

Considering the anonymity of cyberspace, cybercrime may in fact be one of the most dangerous criminal threats ever. A vital component in fighting transnational crime must therefore include the policing of information security and the provision of secure communication channels for police worldwide based on common standards [6].

The effective use (including the sharing) of information is a key priority for the police. Access to information and supporting processes is required for the efficient conduct and management of operations but will be limited to those with a demonstrable need to know and use it who have been appropriately security cleared. In all cases, access to information will be on a least privilege basis. Information and other assets, including supporting processes will be managed and safeguarded to documented levels throughout their lifecycle, including creation, storage, transmission and disposal [3].

Definition of high tech crime offences are defined in Commonwealth legislation within Part 10.7 - Computer Offences of the Criminal Code Act 1995 and include: computer intrusions (for example, malicious hacking), unauthorized modification of data, including destruction of data distributed denial of service (DoS) attacks using botnets the creation and distribution of malicious software (for example, viruses, worms, trojans) [6].

Malicious actors in cyberspace are gaining increasingly sophisticated tools, techniques, and procedures that are outpacing security solutions. Organized criminals and state-sponsored groups now have ample resources to disrupt or breach conventional defenses. Underground hacker markets provide them with ready access to a plethora of products and services. Attackers often rent large botnets or use similar attack tool kits. For instance, the intelligence firm Crowdstrike recently found twelve malicious groups in China using the same exploit codes within 24 to 72 hours of each other. In many cases, malicious attempts to obtain valuable, sensitive data are not isolated, but part of multi-year campaigns. For their victims, the costs of a successful attack can add up in professional services, lost opportunities, and downtime, plus reputation damage, to almost a million dollars [5].

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of

Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology [5].

In conclusion. We are on the frontlines of the fight against cybercrime, and we know first-hand the damage can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data to promote our overall safety [4]. Historically, the security problem have not a high priority in our state. We run the risk of large losses, allowing information to flow and be vulnerable. However, the system must be extremely protected. Protection of information - the priority task of every state. Cybersecurity is extremely important because cyber-attacks can have their origins virtually anywhere in the world, and efforts to control them in most instances will require the cooperation of other states.

Список використаних джерел:

1. Попередження і виявлення високотехнологічних злочинів [Електронний ресурс] / Офіційна веб-сторінка Інтерполу. - Режим доступу: https://www.interpol.int/en
2. Кіберзагрози [Електронний ресурс] / Офіційна веб-сторінка ФБР. - Режим доступу: https://www.fbi.gov/investigate/cyber.
3. Брумнік Р. Терористичні кібератаки та індекс розвитку ІК [Електронний ресурс] / Роберт Брумнік. - Режим доступу : hups.mil.gov.ua
4. Глобальний звіт про погрози [Електронний ресурс] - Режим доступу : https://www.crowdstrike.com/global-threat-report-2015
5. Джейпер Е Скотт. Кіберзагрози США: Механізми обміну розвідданими [Електронний ресурс] / Скотт Е. Джейпер. - Режим доступу: https://www.crowdstrike.com/blog/2015-global-threat-report-preview
6. Міжнародний журнал розвідки і контррозвідки [Електронний ресурс] - Режим доступу : http://www.tandfonline.com/toc/ujic20/current/2016

Mohamed Mohamed Salah Abdelmaksoud
Student, Computer Engineering

Mahyar Tajdini

Student, Information Security

Vlad Kucher

Student, Cyber Security

State University of Telecommunications

MiTM IN PUBLIC NETWORKS (THREATS & RISKS)

MITM[1] Attack

In one of the previous articles of this series, we learnt about various packet spoofing attacks, and also demonstrated how it can result in to a man in the middle attack. However since this attack is most the favored by hackers. As the name suggests, man in the middle attack (references henceforth as MITM) is used mainly to steal information and the data valuable to corporate firms. This attack can be made possible by exploiting inherent vulnerabilities of TCP/IP protocol at various layers, which makes it dangerous. Technically speaking, it is a derivative of packet sniffing and spoofing techniques and if carried out properly, this attack can be completely transparent to the users, thus making it difficult to detect and stop. MITM attack is sometimes referenced as fire brigade attack, eavesdropping attack, or connection hijacking attack.

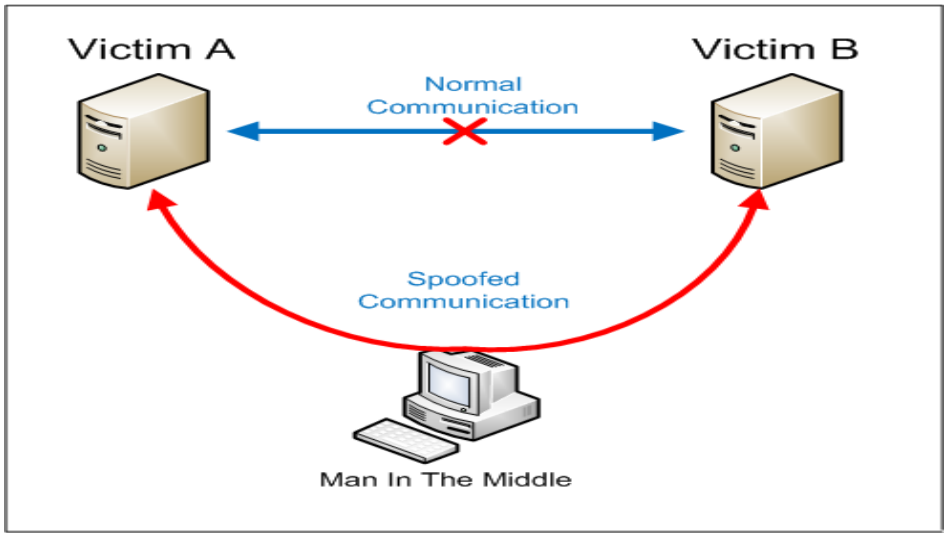


Figure 1

[1]Man in The Middle

Please refer to **Figure 1.** At high level, the steps involved main idea behind MITM are, to intercept traffic, break the authentication chain, and impersonate the hacked endpoints seamlessly. The main objective is to steal the session, and thereby the information being transmitted over the wire. As we know, TCP/IP works on a three way handshake (SYN, SYN-ACK, ACK). This handshake establishes a connection between two different network interface cards, which then use the packet sequencing and data acknowledgements to send or receive data. The data flows from the physical layer all the way up to the application layer. At layer-2 and layer-3, an Ethernet and IP packet datagram are formed, whereas at the presentation layer the cryptographic SSL session is established assuming that the application is planning to use it. It is important to note here, that each of these layers can potentially participate in the MITM attack.

OSI Layer	MiTM Attack Type
Application	Cookie Inject, MITB
Presentation	SSL Hijacking
Transport	IP Spoofing
Data Link	ARP Poisoning, ICMP MiTM

Figure 2

Figure 2. *shows a table which maps the OSI layers to various possible MITM attacks. In order for hacker to steal the session, he needs to use a packet sniffer first. After gathering the packets, he needs to make a choice in terms of which layer to attack in order to gain control, e.g. ARP protocol, or IP or SSL etc. Once the choice is made, hacker then uses advanced tools to inject packets to steal the session and does it so seamlessly that it is transparent to the victims whose session is being hijacked. Although MITM uses IP spoofing at its base, it goes a mile beyond that in order to gain control, by choosing sessions from one or more layers to be hijacked. As an example, the attacker can use ARP spoofing and also cryptographic session stealing to achieve complete control over say an e-commerce transaction. Also as compared to just spoofing the packets, MITM attack modified the intercepted data and re-transmits it over the wire, only this time it makes the victim believe that the packet is legitimate and is coming from a source, which in fact is just another victim.*

As for the impact of MITM attack, since it can happen at various layers, the severity of attack can be very high. As an example, an internal employee can use MITM to download HR database being viewed by a fellow HR employee, by stealing the session of the TCP port being used by SQL server and the HR desktop application. In another example, credit card number could be stolen by hijacking a

browser session connected to a shopping cart web application. Advanced hackers can steal sessions established at the lower OSI such as Layer-3, to dump all the packets flowing and gain a deep dive insight into applications running on that particular computer, and the usage pattern and other personal details of the person using it. It is also possible to record an entire authentication session, and decipher the "username" and "password" information from it, which can be used by hacker to impersonate the victim and create damage to a greater extent. We again wish to emphasize here, that MITM is a transparent attack and hence should be taken very seriously. The good news is that there are few ways to stop or at least mitigate the impact of this attack which we will soon learn. Now let's take a look at various MITM attacks which take place at various networking layers.

ARP Poisoning - *ARP does the MAC address to IP address translation. In a normal and healthy situation, when a TCP/IP protocol stack running on the source computer wants to send a packet to a destination IP address, it first looks into its local cache for a mapping of the IP with a MAC address. If the entry can't be found, it starts an ARP broadcast asking for a MAC address, for the given IP address. The machine who owns that IP address responds back to the ARP query with its own MAC address. The source then uses it to create the Ethernet frame and starts transmission to that IP.*

At the same time, the source machine marks the IP to MAC entry in its local cache, so that it could be used to speed up the communication for future requests to the same IP, by avoiding the broadcasts. ARP is a stateless protocol and also the cache does not have its own security mechanism, which results into a serious vulnerability. The underlying mechanism of MITM being packet spoofing and forging, the attacker sends spoofed ARP packets on the local area network, to associate attackers own machine's MAC address with the IP address of another host which is the target. This forged packet can be as simple as an ICMP packet typically used to Ping a host. The traffic originating for the destination, now in fact reaches attackers machine due to the binding between IP and MAC addresses. Attacker can use the same method to fool another machine, and be able to view communication between both the infected targets, thus making it a local area network specific man in the middle attack.

Once the control is achieved, the hacker simply collects the packet from sender, and forwards it to the receiver while recording the packet stream in between. Since there is no data being lost in this whole process, both the victims has no clue about this, thus helping hacker to hide and yet steal the data. ARP poisoning is widely used in internal attacks whereby a smart hacker or evil guy working on the same local area network can steal sessions which results into a data theft.

ICMP MITM - *In this method, attacker first pings the whole subnet to find out hosts that are down. It maintains a list of such IP addresses and then waits for those hosts to be accessed or pinged by others. When another machine does so, attacker*

responds to it by a successful ping response, which prompts other machines to believe that the host is up, and they start communicating with it for the data transfer. At this point attacker responds to TCP handshakes too, and starts collecting the data. Though this is not completely MITM attack, it does play an important role in data theft. To elaborate better, consider if this would happen with an SQL server or a web server, which would result in loosing userid and passwords, thus breaching the corporate security.

DNS MITM - *This method is rather rarely used, however it can create a serious security breach. An attacker first sniffs the traffic on a network specifically for DNS queries being made on port 53. The information gathered is analyzed to identify all the DNS servers available on the network. The real attack starts here, by using ARP spoofing to fool the querying machine to send DNS requests to attacker's computer, rather than the real DNS server. It is a less known fact, that every DNS query contains a unique identification number as a step towards being able to map it to the response received. In order to establish MITM, a query response packet needs to be created that includes this number, but with a bogus query answer. DNS MITM in real life is a tough thing to execute and also time consuming; however it does leave a great deal of insecurity in the network. What damage could be achieved at this point is up to hacker's imagination. As an example, the hacker can divert all DNS queries asking for IP of a web server, to his own IP addresses, thus creating phishing website and steal information. If this attack is planted externally, the damage can actually be beyond imagination. In another form of DNS MITM attack, the attackers puts DNS server under stress by sending a large number of queries, and in the meanwhile intercept its traffic to respond to the DNS queries by bogus responses.*

DHCP MITM - *Similar to the DNS attack, in this method the DHCP server queries and responses are intercepted. This helps attacker gain complete picture of the network, such as hostnames, MAC addresses, IP addresses and the DNS servers etc. This information is further used to plant advanced attacks to steal the information. Also similar to the DNS attack, an attacker can plant a denial of service attack on a real DHCP server to keep it busy, and in the meanwhile spoof and respond to the DHCP host queries by itself. As we can see, DHCP MITM just acts as a catalyst in the data stealing process, however the impact can further be made severe either by expiring the IP lease on all hosts, thus causing a DHCP broadcast storm on the network, or by assigning same IP to all hosts to cause similar effects. In both of these methods, the network can practically be rendered non-functioning.*

So far we talked about the attacks that take place in the crucial areas of TCP/IP protocol. Now let us talk about the MITM attacks that can happen from the application usage perspective.

Cookie hijacking - *As we know, a cookie is a small piece of text that resides on the user's machine and stores information related to the website that created it. This is usually done to enhance user experience by remembering his online membership*

details or profile settings etc. Since this cookie is stored by a browser, it can be accessed by the browser as well as applications. By writing certain cookie stealing scripts or programs, part of whole of the cookie content can be captured, interpreted and presented to the web server, in order to impersonate the user, who now becomes a victim in this scenario. There are three ways to capture the cookie details, either directly accessing it on the computer, or by hijacking the browser session, or by sniffing the web requests and responses transmitted over the wire. Some websites store login session and authentication information in the cookie, which if hijacked can help attacker login to the server without being challenged for userid and password authentication. The problem created by this situation can be as simple as someone's email account being hijacked, or as severe as someone's online profile being impersonated, thus resulting into possible monetary loss.

Man in the browser - *This is an internet browser attack wherein, a Trojan virus or a malicious script runs in the entity of a browser instance to gain control of the web session. This can be achieved either by exploiting inherent and un-fixed vulnerabilities of an unpatched desktop browser, or by exploiting vulnerabilities which are introduced due to a mis-configuration or non-hardening of the operating system on which the browser is running. Since the attack takes place in the same security context as the user who is using the browser, having security mechanisms such SSL and multi-factor authentication proves to be useless. Multiple operating systems running a variety of browsers exhibit different vulnerabilities, which could be easily exploited by a program written in JavaScript or similar scripting language. To explain the real danger caused by this attack, let's consider a user who is trying to purchase goods on an internet shopping cart using a browser which is already compromised. User sees what is on the screen and submits the request, however what web server sees is what is actually submitted to it, which can be quite different than what was there on the screen. So if a user is submitting the address where the goods are supposed to be shipped to, the address being submitted can be a fictitious one setup by the attacker to collect the goods, while the user who paid for it will not have a clue about it.*

SSL MITM - *As we know, the SSL protocol works on the public key cryptography concepts, whereby a server is hosted with a digital certificate for online data encryption, wherein the certificate is provided by some trusted authority such as VeriSign to endorse the identity of the website URL. In a healthy situation, when a client such as a browser tries to connect to the secure server, the server provides its certificate to the browser. The browser then checks it against its own list of valid and trusted certificates and verifies the information contained in it. Once the certificate is accepted, the server and browser both negotiate on a common level of encryption to be used, create a key and transfer data in the agreed encryption form. If the certificate is expired or non-trusted, the browser flashes a warning to alert the user who is using it. In order to compromise this situation attacker sniffs the traffic between browser and web server, and inserts his computer in the network by using*

standard spoofing techniques. From this point onwards, attacker's computer runs a proxy tool for the SSL communication in such a way that, the web server negotiates SSL key with attacker's machine, while the communication with browser is pure text. This results in exposing all the sensitive information to attacker's computer, which is duly sniffed, recorded and stored for malicious usage. In another case, if the attacker gains physical access to the victim computer temporarily, he installs a bogus certificate on it and then uses IP spoofing to divert the traffic. At this point, attacker uses standard spoofing techniques to be part of the game and establishes SSL connection with web server using the trusted certificate and also with the browser using this bogus certificate. This is done to ensure that web address URL is seen as HTTPS, and the actual communication is indeed SSL helping hacker to hide, but the data is being stolen in the process.

Wireless MITM - *Similar to the wired attacks, in case of wireless networks the data stealing can actually be bit easier. It exploits the design vulnerabilities in the Wi-Fi networks whereby a dummy access point is setup in the network carrying same SSID signature and a stronger signal. The next step is to disrupt client traffic to the real legitimate wireless router, either by spoofing or by subjecting router to the denial of service attack using a packet storm. Once the router gives up, a wi-fi connection is established by the dummy router which starts the packet sniffing and data theft. There are few other ideas such as logging into the real router by using a brute force method and create a wireless bridging with the dummy router, or to fake the MAC address of real router to fool and lure the Wi-Fi clients to dummy router etc. Due to the usage of wireless signals, it is unfortunately possible for hacker to steal data and at the same time be undetected almost forever. Due to lack of knowledge, it is very common to have wireless routers at home or in the network which are not configured correctly or not secured using appropriate keys or passwords.*

Other MITM Attacks - *It is important to note that MITM attacks are possible in the critical networking components as well as new technologies. Routers and managed switches can be spoofed to create a higher security impact, and also the firewalls can be fooled to deliver legitimate traffic to a rough machine. Technologies such as mobile computing and Bluetooth are vulnerable to MITM attacks however those are out of scope for this article.*

Bibliography:

1. Neil DuPaul “Man in the Middle (MITM) Attack // "Vulnerabilities and Prevention”
2. David J. Dodd “Arp Cache Poisoning and Packet Sniffing”
3. HIMANSHU ARORA “ARP Cache Poisoning Fundamentals Explained”
4. Leyden, John (2003-11-07). "Help! my Belkin router is spamming me". The Register.
5. Jump up ^ Meyer, David (10 January 2013). "Nokia: Yes, we decrypt your HTTPS data, but don't worry about it". Gigaom, Inc. Retrieved 13 June 2014.
6. Jump up ^ "NSA disguised itself as Google to spy, say reports". CNET. 12 Sep 2013. Retrieved 15 Sep 2013.

Mohamed Mohamed Salah Abdelmaksoud
Student, Computer Engineering

Mahyar Tajdini

Student, Information Security

Vlad Kucher

Student, Cyber Security

State University of Telecommunications

WHY SHOULD THE INTERNET OF THINGS CARE ABOUT IPV6?

This paper show how it is possible to interconnect different devices, and create interactions between different services. In detail, first, we illustrate the integration of legacy building automation devices into a homogeneous IoT IPv6-based smart office. Then, an advanced scenario regarding building safety is described. And finally, in the last use case, focused on building maintenance, we describes the replacement of a faulty device.

Many answers can be given to such question, and thus, there are several arguments that show IPv6 will be (and actually it is already) a key enabler for the future Internet of Things:

1. *Adoption is just a matter of time*

The Internet Protocol is a must and a requirement for any Internet connection. It is the addressing scheme for any data transfer on the web. The limited size of its predecessor, IPv4, has made the transition to IPv6 unavoidable. The Google's figures are revealing an IPv6 adoption rate following an exponential curve, doubling every 9 months about.

2. *Scalability*

IPv6 offers a highly scalable address scheme. It provides 2^{128} unique addresses, which represents 3.4×10^{38} addresses. In other words, more than 2 Billions of Billions addresses per square millimetre of the Earth surface. It is quite sufficient to address the needs of any present and future communicating device.

3. *Solving the NAT barrier*

Due to the limits of the IPv4 address space, the current Internet had to adopt a trick to face its unplanned expansion: the Network Address Translation (NAT). It enables several users and devices to share the same public IP address. This solution is working but with two main trades-off:

- The NAT users are borrowing and sharing IP addresses with others. Hence, they do not have their own public IP address, which turns them into homeless Internet users. They can access the Internet, but they cannot be directly accessed from the Internet.
- It breaks the original end-to-end connection and dramatically weakens any authentication process.

4. *Strong Security enablers*

IPv6 provides end-to-end connectivity, with a more distributed routing mechanism. Moreover IPv6 is supported by a very large community of users and researchers supporting an on-going improvement of its security features, including IPSec.

5. *Tiny stacks available*

IPv6 application to the Internet of Things has been being researched since many years. The research community has developed a compressed version of IPv6 named 6LoWPAN. It is a simple and efficient mechanism to shorten the IPv6 address size for constrained devices, while border routers can translate those compressed addresses into regular IPv6 addresses. In parallel, tiny stacks have been developed, such as Contiki, which takes no more than 11.5 Kbyte.

6. *Enabling the extension of the Internet to the web of things*

Thanks to its large address space, IPv6 enables the extension of the Internet to any device and service. Experiments have demonstrated the successful use of IPv6 addresses to large scale deployments of sensors in smart buildings, smart cities and even with cattle. Moreover, the CoAP protocol enables the constrained devices to behave as web services easily accessible and fully compliant with REST architecture.

7. *Mobility*

IPv6 provides strong features and solutions to support mobility of end-nodes, as well as mobility of the routing nodes of the network.

8. *Address self-configuration*

IPv6 provides an address self-configuration mechanism (Stateless mechanism). The nodes can define their addresses in very autonomous manner. This enables to reduce drastically the configuration effort and cost.

9. *Fully Internet compliant*

IPv6 is fully Internet compliant. In other words, it is possible to use a global network to develop one's own network of smart things or to interconnect one's own smart things with the rest of the World.

IoT6 use cases

Use case 1: Smart Office and legacy devices Integration

As there still exists a heterogeneous landscape and large variety of legacy devices and networks in the building automation domain, their integration into the Internet through a single interface is still a challenge to face. But, actually it can be addressed by IPv6 and the IoT. In the presented Smart Office scenario, several automation

devices of different legacy networks (i.e., BACnet, KNX) are integrated through a gateway which is responsible for translating legacy protocol messages into IPv6 packages and providing a homogeneous view on the underlying heterogeneous networks and associated devices.

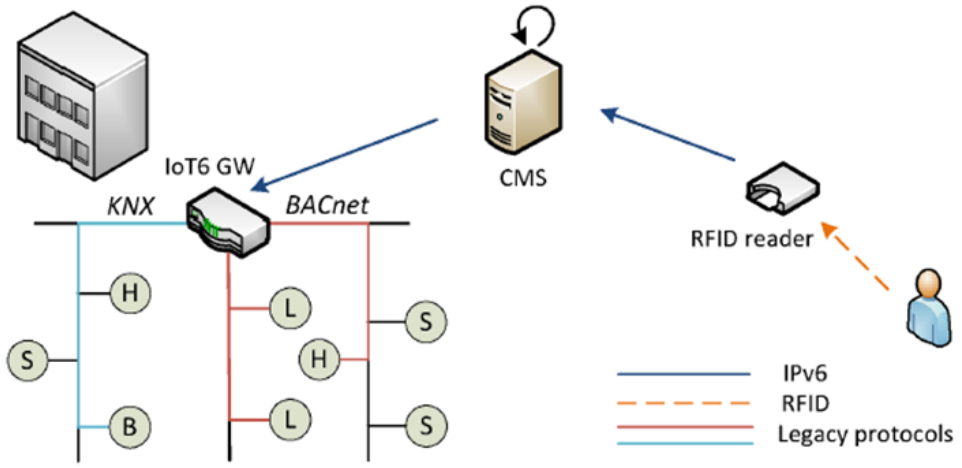


Figure - Use case 1: smart office presence detection

The figure illustrates (i) an IoT6 Gateway (IoT6 GW) integrating several legacy devices, (ii) an IPv6-enabled RFID reader, and (iii) a Control and Monitoring System (CMS) as service in the IoT cloud.

The Smart Office use case starts when an employee enters the building and presents his/her RFID badge to the system's RFID reader. As the RFID reader is IPv6-enabled it may directly communicate with the CMS using IPv6. The CMS subsequently chooses the employee's comfort profile for his/her office and sends settings and commands to the IoT6 GW which integrates devices of the particular office into the IoT. The IoT6 GW controls a variety of different devices from heterogeneous building automation

networks and masks this heterogeneity by providing a uniform IPv6 interface for all devices. The IoT6 Gateway can in further consequence be used to set user-defined preferences for the employee in his/her office. In the example case, the heating actuator set-point (H) and two brightness actuators (L) integrated through a BACnet network are adjusted. At the same time, also the position of the sunblind (B) which is controlled via a KNX network is adapted according to user preferences. For the CMS, the idiosyn-crasies of the different underlying legacy networks make no difference as the IoT6 Gateway transparently integrates these devices into the IoT allowing to adjust them in a uniform way.

A similar situation to the one illustrated in Figure can be observed when the employee leaves the office building. As soon as he/she provides his/her RFID badge to the RFID reader, the CMS is informed that the employee is about to leave the building. In this case, the CMS can execute an energy-saving rule which turns off all

devices in the employee's office. Alternatively, a presence sensor in the office combined with a time-out could be used to detect absence and initiate the energy-saving scenario.

Use Case 2: Safety alert and dynamic routing

The second use case, slightly more complex than the first one, is focused on an emergency situation and the capabilities of an IoT architecture to deal with this. As initial setup for this use case, an IPv6-enabled temperature sensor (S) is considered which periodically sends an update of the sensed temperature value to a Control and Management System (CMS) available as service in the IoT. The starting point for this use case is a sensor that reads a temperature which is too high (i.e., outside the boundaries of usual operation). The Control and Management System detects this abnormality and flags the received message as an alert message. It sends the value to a smart router which is a component in the IoT that according to the type of the message may take different routing decisions. If a normal temperature message is received the smart router sends the temperature messages to a Building Energy Management Server (BEMS) that may be responsible for logging and reporting the energy demand of a building. In the present case (excessive temperature), however, the smart router detects the priority of the message (alert) and according to the tagging carried out by the CMS forwards the value to a specific Safety Server (StS) which is responsible for handling alert situations. As the StS receives the abnormal value it firstly contacts the Global Resource Directory (GRD) to gather information about the location of the sensor. If the StS already has a list of alarm devices with their location it can compare the location of stored devices with the location of the temperature sensor to directly turn on an IPv6-enabled alarm device (A) in the vicinity of the alert situation. If the StS has no pre-stored alarm devices for the area for which the alarm was reported, it is possible to issue another query to the GRD service requesting alarm devices that are in the vicinity (e.g., found in 15 meters radius) of the alert. Any device capable of signaling an alarm which is found can subsequently be switched on. Further, the StS may have a list of mobile phones of persons in charge for alert situations (e.g., fire wardens, system engineers). In this case, the CMS has to gather information about the current location of the IPv6-enabled mobile phones from the Global Resource Directory through an additional query. After it received this information, the CMS can inform responsible persons near the area of interest about the alert situation via their mobile phones. As shown in the Figure, all communication is handled via IPv6 which emphasizes the diversity of devices and components that may be integrated in the IoT. If legacy devices are involved, either on the sensor or on the actuator side, again an IoT6 Gateway can be used for integration as described before.

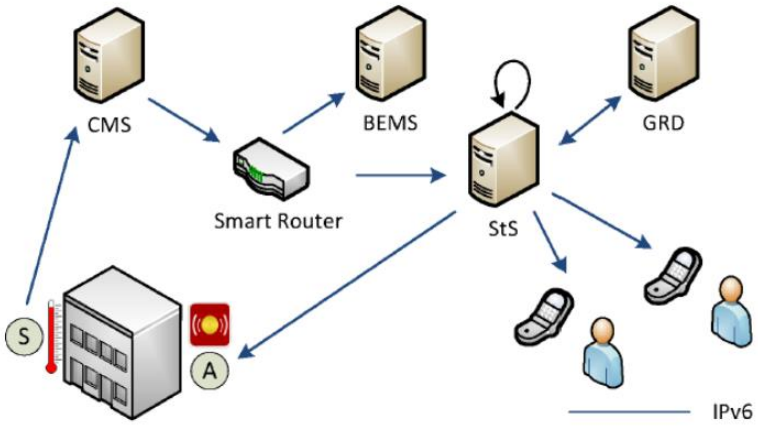


Figure - Use case 2: safety alert

Use case 3: Building maintenance

The third use case is related with building service maintenance. It involves a variety of IoT components and demonstrates how these components in combination with IPv6 communication can be used to detect device failures in a building and investigate as well as fix the cause. In the shown case, a number of sensors are connected to the IoT through an IoT6 gateway (IoT6 GW) which assures that all legacy sensors can be accessed in a uniform way through IPv6 communication (as in the Use Case 1). This use case starts with the failure of a legacy component in the subnet controlled by a specific IoT6 gateway, e.g., a temperature sensor. Usually, a Control and Management System (CMS) observes the value of a temperature sensor to, for example, detect safety situations or perform energy reporting (as in Use Case 2). In the case an observed sensor silently fails, a time-out occurs at the CMS, indicating that something is wrong with the device. A message is generated at the Control and Management System and sent to the Maintenance Tool (MaT) for further examination. In its simplest form, the Maintenance Tool could also run on a local CMS but presently is pictured as global service in the IoT cloud. As soon as the MaT gets the message about the failure of a device, it creates an alert ticket and sends out failure notifications to a variety of mobile phones of responsible persons (e.g., system engineers). The group of recipients may again be based on the current location of the mobile phones for which a lookup call to the Global Resource Directory would be necessary (as in Use Case 2). A person associated with one of the contacted mobile phones seeks out the faulty device and uses a maintenance app on the mobile phone to scan its RFID tag. The information is relayed to the MaT which needs to find out the device which is associated to the respective RFID tag. Therefore, it queries the Global Resource Directory (GRD) for the location of the Smart Things Information Service (STIS), a database-like service that keeps associations between RFID tags and devices. The MaT further sends back information to the maintenance app running

at the mobile device providing the system engineer with more information about the device. With the help of this information, the engineer has the possibility to run diagnostics on the device. In this case, the CMS further acts as an intermediary between Maintenance Tool and the IoT6 Gateway, accepting and relaying messages from the Maintenance Tool to the IoT6 Gateway. In case the device's defectiveness is confirmed, a replacement order needs to be made. This order can again be performed using the MaT. The information previously retrieved from the STIS may in this case further be used to directly order the spare part from an Inventory Management System (IMS), another service in the IoT. If the address of the IMS is not yet known by the MaT, it first again has to issue a request to the GRD. Alternatively, the IMS may be part of the maintenance tool in which case the separation of the two services can be omitted.

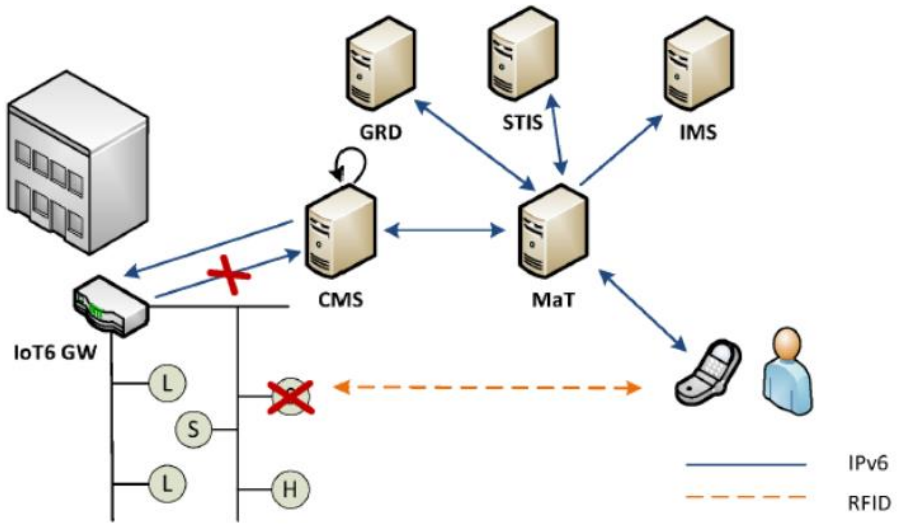


Figure - Use case 3: building maintenance

IPv6 advantages for IoT

IPv6 is good for IoT and IoT is good for IPv6. There are several arguments and features that demonstrate that IPv6 is actually a key communication enabler for the future Internet of Things:

- Adoption is just a matter of time

  The Internet Protocol is a must and a requirement for any Internet connectivity. It is the addressing scheme for any data transfer on the web. The limited address capacity of its predecessor, IPv4, has made the transition to IPv6 unavoidable. Google's figures are revealing an IPv6 adoption rate following an exponential curve, doubling every 6 months.

- Scalability

  IPv6 offers a highly scalable address scheme. The present scheme of Internet Governance provides at most 2 x 10^{19} unique, globally routable, addresses.

This is many orders of magnitude more that the 2 x 10^9 that is possible with IPv4 and the 10^{13} that is the largest estimate of IoT devices that will be used this century. It is quite sufficient to address the needs of any present and future communicating device still allowing it to have many addresses.

- Solving the NAT barrier

  Due to the limits of the IPv4 address space, the current Internet had to adopt a stopgap solution to face its unplanned expansion: the Network Address Translation (NAT). It enables several users and devices to share the same public IP address. This solution is working but with two main trades-off:

  The NAT users are borrowing and sharing IP addresses with others. While this technique allows single stakeholders to mount large applications, it becomes completely unmanageable if the same end-points are to be used by many different stakeholders; this would occur in an IoT deployment where the same sensors are to be used by multiple, independent, stakeholders. Secondly the mechanism cannot be used to access specific end-points from the Internet..

- Multi-Stakeholder Support

  IPv6 provides for end devices to have multiple addresses and an even more distributed routing mechanism than the IPv4 Internet. This allows different stakeholders to assign IoT end-device addresses that are consistent with their own application and network practices. Thus multiple stakeholders can deploy their own applications, sharing a common sensor/actuation infrastructure, without impacting the technical operation or governance of the Internet.

- IPv6 Features

Many features have been built into the basic IPv6 specifications that are very useful both for the operation and the deployment of IoT. Besides the features already mentioned, these include multicast, anycast, mobility support, auto-configuration and address scope.

- Over the last decade, many new higher level protocols have been developed that are both useful for IoT and are well-suited to devices with constrained resources. Examples are 6LowPAN (wireless nets), COAP (transport with web services) and DTLS (secured datagrams). Indeed there is a whole REST environment targeted at constrained devices.

- Tiny operating systems and network stacks

IPv6 application to the Internet of Things has been researched for many years. The research community has developed several operating systems like TinyOS and Contiki that are relatively small and support the above protocol suites and environments. While the main IPv6 is very rich in possible features, these reduced environments have often restricted carefully the features available in order to meet IoT needs while reducing the size of the underlying system and leaving more space for applications. For example a basic Contiki system takes less than 20KByte, and

even one supporting a full IPv6 stack and the other high-level protocols including DTLS can probably fit into 70 Kbyte

- Increased hardware support

The operating system and network stack (with security) could be made much more compact by providing more hardware support in the chipset (or a co-processor). However such initiatives would detract from the efficient porting of the system to other chipsets. It would be desirable to make such upgrades for large deployments in commercial environments.

- Mapping of physical systems onto IPv6 address and Privacy extension

  We have shown it is possible to map many features of the physical IoT devices onto IPv6 addresses. This can ease large-scale deployments – though at the cost of revealing to anyone interested architectural features of the IoT devices because of the transparency of the Domain Name Service entries.

  In contrast, IPv6 provides for privacy by automatically randomizing the suffix of the IPv6 address to hide the MAC address or any serial number used as identifier when connecting to the Internet. This feature is made available on all operating systems automatically.

  Of course these two techniques have contradictory aims and effects; their relevance are determined by the needs of the IoT application.

- Use of Identifiers and improved functionality

We have shown that by the use of Identifiers in conjunction with IPv6, one can take advantages of IPv6 features without their drawbacks. For example, with systems like Handle the structure can mirror the topology of a deployment, while the security features of the identifier system precludes unauthorized access to this information. At the same time IPv6 addresses can be attributes of the Handle Identifiers, but use the privacy enhancements at the same time.

- Enabling the extension of the Internet to the web of things

  Thanks to its large address space, IPv6 enables the extension of the Internet to any device and service. Experiments have demonstrated the successful use of IPv6 addresses to large-scale deployments of sensors in smart buildings, smart cities and even with cattle. Moreover, the CoAP protocol enables the constrained devices to behave as web services easily accessible and fully compliant with REST architecture.

- Mobility

  IPv6 provides strong features and solutions to support mobility of end-nodes, as well as mobility of the routing nodes of the network. The project has also achieved some interesting results on including Mobile IP in the Contiki stack.

- Address auto-configuration

  IPv6 provides an address self-configuration mechanism (Stateless mechanism). The nodes can define their addresses in very autonomous manner. This

enables drastic reduction of IoT configuration effort and deployment cost. With an Identifier-based system like Handle, this technique can be combined with automated procedures to derive authentication tokens from the device, and have access control features added.

- Fully Internet compliant Gateways

IPv6 Gateways can be fully Internet compliant. In other words, it is possible to build a proprietary network of smart things or to interconnect one's own smart things with the rest of the World via a gateway that is fully compliant with IP requirements towards the Internet.

- Standardization

Some of the IoT6 developments like GLowBALIP and the Identifier system would benefit hugely if their attributes were standardized in this context much more rigidly for IoT. EC initiatives should support directly such standardization – possibly in a Support Action..

- Dissemination

Much detailed dissemination has been achieved in IoT6. However applicability to new applications by new entities would require even more dissemination. Again this activity could be included in a further Support Action.

Mohamed Mohamed Salah Abdelmaksoud
Student, Computer Engineering

Mahyar Tajdini

Student, Information Security

Vlad Kucher

Student, Cyber Security

State University of Telecommunications

ANTIVIRUSE AND FIREWALL ARE NOT ENOGH

Antivirus software is widely used to protect data. It is believed that antiviruses are the dominant means of securely protecting a computer and of offering safer access to the internet. Because of the fact that antivirus programs are very complex forms of software, we are not going to analyze them in great detail. We are just going to present in a simple manner the way they detect malware and what must be avoided to bypass detection.

Antivirus

A variety of strategies are typically used for malware detection.

1. **Signature-based detection:** Traditionally, antivirus software heavily relied on signatures to identify malware. Signature-based detection involves searching for known patterns of data within executable code. This can be very effective, but cannot protect against malware unless samples have already been obtained and signatures created. As a result of this, signature-based approaches are not effective against new, unknown malwares.

Although the signature-based approach can effectively contain malware outbreaks, it is possible for a computer to become infected with new malware for which no signature is yet known and malware is often modified to change its signature without affecting functionality. The use of metamorphism and polymorphism from malware writes is widely used.

2. **Heuristics:** Another technique used in antivirus software is the use of heuristic analysis to

identify new malware or variants of known malware.Many viruses start as a single infection and through either mutation or refinements by other attackers, can grow into dozens of slightly different strains, called variants. Generic detection refers to the detection and removal of multiple threats using a single virus definition.

While it may be advantageous to identify a specific virus, it can often be more efficient to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded withextra, meaningless code. A detection that uses this method is said to be "heuristic detection."

3. **Real-time protection:** Newer antivirus software also has another mechanism called “real time”

protection. It is known that some (malicious) code may be hidden, encrypted, obfuscated or even created instantly. To be able to deal with such tricks antivirus packages are also capable of monitoring and intercepting API calls and of performing a kind of "behavioral analysis". So, if a well-known process acts in an unusual manner the antivirus will mark it as suspicious.

4. **Virus database update**: It should be clear by now that virus databases require continuous update by the vendor. There are several ways that Antivirus (AV) vendors are notified of new malicious files. We will not discuss all of them but the general idea behind this process will be illustrated.

One source is from online file scanner sites where people upload a file they consider to be suspicious, and want to ascertain if it is actually a virus or not. They upload their files to one ofthese sites to check which antivirus packages detect it and, subsequently flag it as a virus. Once the files are uploaded,based on certain elements, they are then distributed to the antivirus vendor's labs.

Another way of vendor notification is by the antiviruses themselves. Almost every antivirus software has an option already checked and recommended (by the AV vendors) to participate in their grid. With this option enabled the antivirus will automatically send the files out when any file is detected

as suspicious. Antiviruses also include the option to send off a file to the vendor with just a click of abutton through their platform. If the file is analyzed and identified as malware, its signature will be added to the dictionary.

After this presentation of antivirus software methodology the ways in which we can avoid detection should be apparent. The steps that we have followed for our crypter are the following:

Unique crypter's code: In our implementation, we have not included code snippets from formerly used (already detected) crypters. All the function has been rewritten in a different and unique way.

Deactivation of auto distribution or test offline: For testing purposes we needed an antivirus to always check our implementation. In order to prevent the distribution of our crypter, we deactivated the auto distribution option and later on we blocked the antivirus access to the internet.

Not scanning on online sites that redistribute: For testing purposes we needed to test our crypter in as many antiviruses as possible. This was not an easy task because of limited resources so we were oblged to use an online scanner. On some online scanners there is an option available to check for no distribution but it is important to confirm its trustworthiness.

Bypassing Antiviruses

Antiviruses are a big annoyance for hackers. When a hacker wants to penetrate a system, the success or failure of that hack often depends on whether the target computer has an antivirus or not. Thus, bypassing antiviruses are naturally a hot topic among hackers. Although there are no fool-proof methods to bypass antivirus,

1. **File Splitters and Hex editors**

The first technique that we are going to discuss is using file splitting tools to identify the exact signature that is being detected by the antivirus application and modify it. This is one of the oldest ways to bypass AV tools. This technique is efficient if we can locate the exact signature that is being detected. However, there is a limitation with this

technique. If messing the functionality of the application, it becomes useless even if bypassing antivirus.

This can be achieved by using a file-splitting tool to split the binary into many parts. This splitting should be done in such a way that each part is larger than the previous one by a fixed amount. Then just need to run the Antivirus scan on these parts to identify which part is flagged first as malicious.

2. Metasploit polymorphic encoder

The metasploit framework comes with an excellent set of tools that includes a polymorphic encoder that can "encode" any trojan or virus such that antiviruses would not be able to recognize its signature, thus avoiding detection. The best encoder under msfencode is shikata ga nai, which can be used to "encode" and obfuscate your payload(read trojan) multiple times.

In computer terminology, polymorphic code is code that uses a polymorphic engine to mutate while keeping the original algorithm intact. That is, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all. For example, 1+3 and 6-2 both achieve the same result while using different code. This technique is sometimes used by computer viruses, shellcodes and computer worms to hide their presence.

Encryption is the most common method to hide code. With encryption, the main body of the code (also called its payload) is encrypted and will appear meaningless. For the code to function as before, a decryption function is added to the code. When the code is executed this function reads the payload and decrypts it before executing it in turn.

Encryption alone is not polymorphism. To gain polymorphic behavior, the encryptor/decryptor pair are mutated with each copy of the code. This allows different versions of some code which all function the same

3. Crypters/Packers

Crypters and packers are specialized tools that can encrypt and pack your payload(read trojan or virus) so that antivirus cannot get to the actual core of the payload. The encryption on the payload prevents antiviruses from peeking inside. Because of this, antiviruses will not detect your trojan. Once ready to deploy the trojan, the payload gets unencrypted and unpacked to unleash all malicious activities and infections.

4. Binary editing

Antiviruses use file signatures to detect viruses. These file signatures are unique patterns inside the virus. They are very small(a few dozen bytes). Binary editing involves finding the file signatures and directly altering it. Once the contents of the file signature are changed, the antivirus will no longer recognize the signature.This can be done using a Hex Editor.

5. Modify Source code

If the source code of the program/virus is available, with modification can bypass antiviruses. For instance, If there is a switch case condition in the code, convert it into

if-else. This should not affect the functioning of the program in any significant way. There are many other changes that can make, like changing variable names, upper to lower case etc.

int num=0;

can be changed to

int NUm=0;

6. **Recompile the payload/Use an alternate version**

If the source code of the virus are available, then recompile that with a different compiler. It will create a completely fresh executable. That way, there is a chance that the antivirus will no longer recognize the signature.

Bypassing Firewalls by Reverse Connection

A reverse connection is usually used to bypass firewall restrictions on open ports. A firewall usually blocks incoming connections on open ports, but does not block outgoing traffic. In a normal forward connection, a client connects to a server through the server's open port, but in the case of a reverse connection, the client opens the port that the server connects to. The most common way a reverse connection is used is to bypass firewall and router security restrictions.

For example, a backdoor running on a computer behind a firewall that blocks incoming connections can easily open an outbound connection to a remote host on the Internet. Once the connection is established, the remote host can send commands to the backdoor. Remote administration tools (RAT) that use a reverse connection usually send SYN packets to the client's IP address. The client listens for these SYN packets and accepts the desired connections.

If a computer is sending SYN packets or is connected to the client's computer, the connections can be discovered by using the netstat command or a common port listener like “Active Ports”. If the Internet connection is closed down and an application still tries to connect to remote hosts it may be infected with malware. Keyloggers and other malicious programs are harder to detect once installed, because they connect only once per session. Note that SYN packets by themselves are not necessarily a cause for alarm, as they are a standard part of all TCP connections.

There are honest uses for using reverse connections, for example to allow hosts behind a NAT firewall to be administered remotely. These hosts do not normally have public IP addresses, and so must either have ports forwarded at the firewall, or open reverse connections to a central administration server.

Маковій Вікторія Володимирівна, аспірант
Державний університет телекомунікацій
Навчально-науковий інститут
менеджменту та підприємництва
кафедра Менеджменту
м. Київ

СУТНІСТЬ ТА ЗМІСТ ІНФОРМАЦІЙНОГО МЕНЕДЖМЕНТУ

Розкрито зміст та сутність понять «інформація» та «менеджмент» як системоутворюючих складових поняття «інформаційний менеджмент». Визначено мету інформаційного менеджменту. Вказано основні завдання які виконує інформаційний менеджмент на підприємстві.

У сучасних умовах розвитку економічного суспільства та підприємницької діяльності значно посилюється роль інформації. Ефективний та успішний менеджмент підприємства базується на своєчасно отриманій достовірній інформації. Компетентність сучасного керівника залежить не стільки від досвіду, отриманого в минулому, скільки від володіння достатньою кількістю актуальної для даної ситуації інформації та вміння зробити своєчасні висновки. Тобто прийняття будь-якого рішення вимагає оперативної обробки значних масивів інформації. Розв'язанням цієї проблеми займається інформаційний менеджмент. Однак, ефективна практична реалізація інформаційного менеджменту на підприємстві є можливою лише за існування чітко визначеної теоретичної основи.

Поняття «інформація» і «менеджмент» є системоутворюючими складовими поняття «інформаційний менеджмент».

Поняття «інформація» має безліч значень. Розглянемо деякі з них [1, с.6]:

- Інформація - це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі.
- Інформація - відомості про оточуючий світ і процеси, щоу ньому відбуваються, які сприймаються людиною або спеціальним пристроєм.
- Інформація - універсальна субстанція, яка пронизує всі сфери людської діяльності, слугує провідником знань і думок, інструментом спілкування, взаєморозуміння і співробітництва

Термін «менеджмент» вживається у багатьох значеннях і часто застосовується як синонім терміну "управління". Дослідниками науки управління наведено множину понять "менеджмент" і " управління" – від розуміння менеджменту як складової управління, до ототожнення цих понять [1, с.7]. Наприклад, Оксфордський словник англійської мови дає такі його тлумачення:

- Менеджмент – це вміння й адміністративні навички організовувати ефективну роботу апарату (служб працівників).

- Менеджмент – це органи управління, адміністративні одиниці, служби і підрозділи.

Нерідко менеджмент трактується як сукупність методів, принципів, функцій, засобів, і форм управління підприємствами, з метою реалізації стратегічних планів, досягнення ефективності виробництва і збільшення прибутку.

Менеджмент, як процес, здійснює управління реальним об'єктом з метою одержання максимальних результатів. На першому етапі процесу управління здійснюється збір і нагромадження інформації про стан об'єкта управління й зовнішнього середовища, на другому - її обробка для прийняття управлінських рішень. Третій етап процесу управління передбачає видачу й доведення до об'єкту управління розпоряджень (команд).

Розуміння інформаційного менеджменту можна обмежити двома значеннями:

- управління інформацією – інформаційними потоками й інформаційними ресурсами, тобто, автоматизована технологія обробки інформації в певній предметній області;

- управління за допомогою інформації, тобто управлінська технологія, менеджмент у власному змісті цього слова.

Для розуміння суті інформаційного менеджменту необхідно звернути увагу на деякі важливі положення:

1. інформація — це засіб ділового спілкування;
2. інформація – засіб доведення до суспільства відомостей про підприємство;
3. інформація – це джерело відомостей про внутрішнє та зовнішнє середовище;
4. інформація – це товар;
5. інформаційний менеджмент здійснюється в межах конкретного підприємства;
6. інформаційний менеджмент має відношення не просто до інформації, а до інформаційної діяльності організації.

Слід відмітити, що загальною метою інформаційного менеджменту є виробництво потрібної для організації інформації для забезпечення ефективного управління всіма її ресурсами і створення необхідного інформаційного програмного і технічного середовища для здійснення управління організацією.

Інформаційний менеджмент вирішує завдання планування, керівництва, контролю й організації документаційного забезпечення управління підприємством за певними цільовими критеріями для підтримки узгоджених організаційно-інформаційних дій.

Важливим завданням інформаційного менеджменту є вибір раціональних форм комунікацій, техніки й інформаційних технологій, а також характеристик інформаційних ресурсів, необхідних для досягнення цілей підприємства.

Інформаційний менеджмент на підприємстві виконує стратегічні, оперативні та адміністративні задачі. До числа стратегічних задач відносяться створення інформаційної інфраструктури підприємства та управління інформаційними технологіями. Оперативні та адміністративні задачі носять більш обмежений і підлеглий характер.

Варто наголосити на тому, що інформаційний менеджмент базується на використанні інформаційних технологій. Для того, щоб інформаційні технології підвищували ефективність управлінського процесу й сприяли розвитку організації, а не протидіяли йому, необхідно забезпечити легкий і доступний обмін інформацією для всіх учасників діяльності. Для цього інформацію треба сприймати, розуміти, тобто володіти комунікативними властивостями.

Інформаційний менеджмент як наукова категорія пройшов тривалий період розвитку. Наукові підходи змінювалися, доповнювались, однак і на сучасному етапі розвитку наукової думки єдиного підходу до трактування поняття «інформаційний менеджмент» немає.

Література:

1. Матвієнко О. В. Інформаційний менеджмент: опорний конспект лекцій у схемах і таблицях / Матвієнко О. В., Цивін М.Н. - К. : Слово, 2007. – 200 с.

Галіцька Яна Анатоліївна
Державний університет телекомунікацій
Навчально-науковий інститут
менеджменту та підприємництва
м. Київ

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

У сучасних умовах глобалізації інвестиційний розвиток держави є важливим чинником її загального розвитку. В умовах, коли економіка України відчуває значну нестачу інвестиційних ресурсів, питання розробки ефективної інвестиційної політики набуває особливої актуальності. При цьому значну увагу потрібно приділяти іноземним інвестиціям. Іноземний капітал (інвестиції) ефективно впливає на економічний розвиток господарства країн, які імпортують його. Перевагами таких грошових надходжень є те, що, по-перше, іноземні інвестиції – це додатковий капітал, залучений у країну для виробництва товарів і послуг, реалізації певних програм, а по-друге – це надходження в державу нових технологій та застосування нових методів управління. Крім того, іноземні інвестиції сприяють створенню в країні нових робочих місць, вирішенню нагальних соціальних проблем.

На даний час сфера телекомунікацій є однією з найважливіших складових інфраструктури в Україні. Відповідно інвестиційне забезпечення розвитку даної сфери є передумовою підвищення конкурентоспроможної

національної еконо- міки, що, у свою чергу, сприятиме входженню нашої країни у глобальний економічний простір.

На сучасному етапі широкосмугові технології стали не просто засобом передачі даних, а істотним чинником забезпечення сприятливих умов для розвитку системи державного управління, економіки, науки, освіти та культури, у тому числі надання адміністративних послуг.

Інвестиції в галузь зв'язку України дозволять вирішити такі існуючі проблеми, як: забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання; впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень; дослідження, розробка та впровадження нових принципів органі- зації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Інвестиції, у тому числі іноземні, є не лише механізмом розвитку, але й способом регулювання економіки шляхом переливання капіталу. На сучасному етапі розвитку ринку іноземні інвестиції виступають основним джерелом отримання новітніх конкурентоспроможних технологій. Залучення інвестицій – це необхідна умова розвитку всіх галузей економіки, особливо сфери телекомунікацій, що є інноваційною за своєю суттю. Інвестиційна дія- льність операторів телекомунікацій сприятиме збільшенню обсягів послуг сфери телекомунікацій в Україні і підвищенню їх якості, а також розвитку та модернізації телекомунікаційної мережі. Разом з удосконаленням законодавства щодо іноземних інвестицій повинні розвиватися й інші чинники механізму залучення іноземних інвестицій. Необхідно забезпечити стабільність політичного середовища, вдосконалити та забезпечити стабільності: податкової, грошово-кредитної та митної політики; максимально спростити процедури, які регламентують взаємовідносини між державою і підприємцями в галузі залучення іноземних інвестицій; створити гарантії стабільності умов щодо довгострокового фінансування інвестиційних проектів, здійснити вдосконалення системи захисту прав інвесторів; удосконалити роботу інститутів спільного інвестування; запровадити дієвість страхування інвестиційних ризиків. Отже, створення сприятливих умов для залучення іноземного інвестування є найважливішою складовою серед тих економічних вимог, які покликані забезпечити реальні зміни в економічній структурі суспільства, надати поштовх усьому ланцюгу господарських взаємозв'язків цілісного процесу суспільного відтворення, спрямованого на розвиток економіки України.

Література:
1. Гилка У.Л. Особливості конкуренції на ринку послуг телекомунікацій: [Текст] / Гилка У.Л. // Наукові записки УНДІЗ. – 2009. – №3(11). – С. 95-103
2. Діденко Я.О. Удосконалення прямого іноземного інвестування: [Текст] / Діден- ко Я.О // Фінанси України. – 2004. – №12. – С. 96-105.
3. Підсумки роботи галузі: [Електронний ресурс]. – Режим доступу:http://www.stc.gov.ua/uk/publish/article/63905.

Андрієнко Олеся Григорівна
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

ІНФОРМАТИКА - БАЗОВИЙ ПРЕДМЕТ ДЛЯ ВИВЧЕННЯ НА ПЕРШОМУ КУРСІ

I. Постановка проблеми

I.I. Загальні положення про інформатику. Термін "інформатика" походить від французьких слів *information* (інформація) і *automatique* (автоматика) і дослівно перекладається як "інформаційна автоматика". Інформатика - це заснована на використанні комп'ютерної техніки дисципліна, вивчаюча структуру і загальні властивості інформації, а також закономірності і методи її створення, зберігання, пошуку, перетворення, передачі і прийому в різних сферах людської діяльності.

I. II. Актуальність даної теми. Процес дослідження інформатики, алгоритмів, базових навичок в програмуванні та їх теоретичних складових актуалізує широке коло професійних, методологічних і навчальних проблем, пов'язаних із пізнанням загальних закономірностей та структури розвитку наукового потенціалу і базових знань. Дана галузь суттєво рухається вперед і розвивається та дає нам нові уявлення про досягнення в науці, зокрема, в інформатиці. Тож можна сміливо сказати, що сьогодні без врахування наукового внеску, знання базових навичок з інформатики не може обійтись жодна серйозна робота.

I.III. Розглянуті питання. В роботі розглянуто декілька важливих питань, а саме:

- Важливість предмету інформатика на першому курсі у ВНЗ. Порівняння у вивченні інформатики в інших ВНЗ.
- Важливість вивчення алгоритмів до вивчення мов програмування високого рівня.
- Де очікується можливе застосування придбаних під час навчання знань і навиків.

II. Мета

Оскільки зараз практично всюди використовується автоматика в управлінні і роботі найрізноманітніших систем і галузей, котрі побудовані і виконуються за певною програмою, яка в свою чергу працює за конкретним алгоритмом. Саме тому, метою статті є подальший розгляд предмету, який повинен викладатися з першого курсу та висвітлення позитивних аспектів даної теми.

III. Виклад основного матеріалу

Пріоритетні напрямки інформатики це:

- розробка обчислювальних систем і програмного забезпечення;
- теорія інформації, вивчаюча процеси, зв'язані з передачею, прийомом, перетворенням і зберіганням інформації;
- математичне моделювання, методи обчислювальної і прикладної математики;
- методи штучного інтелекту;
- системний аналіз;
- соціальна інформатика;
- телекомунікаційні системи і мережі.

Прогресивне збільшення можливостей комп'ютерної техніки, розвиток інформаційних мереж, створення нових інформаційних технологій приводять до значних змін у всіх сферах діяльності суспільства: в промисловості, науці, освіті, медицині. Для початку формування свідомості про дану галузь, потрібно вводити цю дисципліну з першого курсу, щоб засвоїти початкові знання і уявлення про вибрану спеціальність.

Алгоритмом називають зрозуміле і точне розпорядження виконавцю про виконання послідовності дій, спрямованих на досягнення зазначеної мети чи на вирішення поставленої задачі. Алгоритмічне мислення допомагає чітко побачити кроки, що ведуть до мети, замітити всі перешкоди і уміло їх обійти. Система "Алгоритм" відноситься до складу автоматизованого візуального проектування і представляє собою інтегрований осередок, який дозволяє перетворювати, відображувати, налаштовувати і безпосередньо виконувати різні алгоритми. Застосування даної програми дає вагомий внесок у вивченні інформатики і подальшому вивченні мов високого рівня програмування.

Отриманні знання, навики і досвід в роботі можна застосовувати в різних сферах. Як повідомляє інформаційний портал програмістів і працівників сфери IT сайт DOU, заробітна плата на посаді DevOps за III квартиль складає 3000 доларів. Вивчення різних мов програмування дає можливість хорошого кар'єрного росту, це якщо говорити за фінансову сторону питання. Потребують спеціалістів, які можуть швидко налагодити і мінімізувати затрати на роботу певної промисловості дуже цінуються. Застосування знань в інформатиці

можна відобразити і в покращені вже існуючих програм, створенню нових ідей і у вирішенні глобальних проблем.

Висновки

Впровадження в систему навчання у вищих навчальних закладах такого предмету як "Інформатика" на першому курсі є досить вдалим кроком до поліпшення вивчення як свої спеціальності так і покращення рівня своєї освіти студентами. Цю методику, на мою думку, потрібно застосовувати, адже ми живемо в інформаційному суспільстві і це є одним і вагомих аспектів нашого життя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації з дисципліни "Інформатика" для 1 курсу, Державний університет телекомунікацій.
2. Інформатика [Електронний ресурс] // Поняття алгоритмів, властивості алгоритмів - Режим доступу: https://stboinf.wordpress.com
3. DOU [Електронний ресурс] // Статистика зарплат програмістів в Україні

Чижевська Марія Анатоліївна
Державний університет телекомунікацій
Факультет Інформаційних Технологій
м. Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ MIMO У СУЧАСНИХ МЕРЕЖАХ

Застосування технології MIMO є важливим завданням для реалізації багатоканальної системи передачі інформації при наявності багатьох джерел радіосигналів. Технологія MIMO збільшує смугу пропускання сигналу за рахунок використання декількох антен для передачі та прийому та використовується у бездротовому зв'язку Wi-Fi, WiMAX, LTE для більш ефективного використання частотної смуги.

MIMO (Multiple Input Multiple Output: множинні входи, множинні виходи) - метод просторового кодування сигналу, що дозволяє збільшити смугу пропускання каналу, при якому для передачі та прийому даних використовуються дві і більше антени. Технологія MIMO дозволяє в одному частотному діапазоні передавати більше даних. Головним способом досягнення зазначених вище переваг є передача даних від джерела до одержувача через кілька радіо з'єднань.

Технологія MIMO використовується у бездротовому зв'язку Wi-Fi, WiMAX, LTE для збільшення пропускної спроможності і більш ефективного використання частотної смуги.

Використання даної технології у безпровідних мережах дозволяє вирішити такі проблеми, як постійно зростаюча інтерференція, обмежена смуга пропускання і недостатній радіус дії. Крім того, передача інформації паралельно по декількох каналах підвищує надійність з'єднання.[1, с.206]

Розповсюдження хвиль при передачі сигналу

В умовах щільної забудови, через велику кількість перешкод, виникає ситуація, коли між абонентським обладнанням і антенами базової станції відсутня пряма видимість. У цьому випадку, єдиним варіантом досягнення

сигналу приймача є відбиті хвилі. Якщо при розповсюдженні сигналу прямої видимості немає, то хвиля йде до пункту призначення кількома шляхами і відповідно кожен промінь проходить різну відстань. Однак, багаторазово відбитий сигнал уже не має вихідної енергії і може прийти із запізненням.

SU-MIMO та MU-MIMO

Спочатку технологія MIMO була розрахована на роботу з одним користувачем і називалася SU-MIMO (Single User MIMO). У SU-MIMO вся пропускна здатність маршрутизатора віддавалася одному пристрою, максимізуючи його швидкість передачі даних. На противагу SU-MIMO, обмеженою одним клієнтським пристроєм, технологія MU-MIMO може працювати з декількома клієнтами.

Найпростіша антена MIMO

Найпростіша антена MIMO - це система з двох несиметричних монополей, орієнтованих під кутом ± 45 ° щодо вертикальної осі.

Аналогічна антена використовується і на приймальній стороні. Такий підхід дозволяє одночасно передавати сигнали з однаковими несучими, модульованими різним чином. [3]

Конфігурації технології MIMO

У стандарті 4G можливе застосування технології MIMO з конфігурацією до 8x8. Теоретично це дозволить транслювати цифровий потік від основної станції до отримувача на швидкості більше 300 Мбіт/с.

Для роботи технології MIMO необхідні деякі зміни у структурі передавача в порівнянні зі звичайними системами: на передавальній стороні необхідний дільник потоків, який буде розділяти дані, призначені для передачі на кілька підпотоків, число яких залежить від числа антен.

Наприклад, для MIMO 2x2 і швидкості надходження вхідних даних близько 100 Мбіт/с дільник буде створювати 2 потоки по 50 Мбіт/с кожен. Далі кожен з даних потоків повинен бути переданий через свою антену. В одному з можливих способів організації технології MIMO сигнал передається від кожної антени з різною поляризацією, що дозволяє ідентифікувати його при прийомі.

Наразі шукають шляхи для розробки нових конфігурацій MIMO антен до 64x64. У майбутньому це дасть можливість ще більше поліпшити ефективність спектральних показників, збільшити ємність мереж і величину швидкості транслювання інформації.[4]

Отже, технологія MIMO дуже швидко завоювала популярність за рахунок збільшення ємності і пропускної здатності протоколів передачі даних та знайшла практичне застосування в бездротових локальних мережах стандарту IEEE 802.11n, а також в бездротових мережах мобільного зв'язку WiMAX і LTE.

Література:

1. А.Н. Дубик, В.И. Слюсар, А.А. Зінченко Системи цифрової обробки сигналів. –П.: Полтавський військовий інститут зв’язку. – С. 206

2. Г.С. Джобалаєва, А.Ж. Сагиндікова, К.Н. Тайсарієва, О.Е. Боранбаєва, А.Б. Мирзаханов Использование технологии MIMO в сетях LTE. – С. 5

3. http://3g-aerial.biz/chto-takoe-mimo-antenna
4. http://antenna31.ru/?p=3723

Водько Андрій Романович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ЗНАЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЖИТТІ СУЧАСНОЇ ЛЮДИНИ

Більшість з нас вже не уявляють жодного дня без комп'ютера. Зі стрімким розвитком технологій доступнішими стають різноманітні пристрої, що спрощують життя людей. Це стосується й сучасних комп'ютерів, які спроможні забезпечити вражаюче швидку обробку інформації.

Комп'ютери з їхніми вражаючими здібностями задіяні в багатьох сферах. «Розумні» механізми використовуються й для освоєння підводного світу, і для розкриття таємниць космосу. Головне – застосовувати інформаційні технології на благо людства, адже саме ми вирішуємо, у яке русло направити ці можливості – позитивне або негативне.

В умовах розвитку сучасного суспільства інформаційні технології глибоко проникають в життя людей. Вони дуже швидко перетворилися на життєво важливий стимул розвитку не тільки світової економіки, а й інших сфер людської діяльності. Зараз важко знайти сферу, в якій зараз не використовуються інформаційні технології. Так, у промисловості інформаційні технології застосовуються не тільки для аналізу запасів сировини, комплектуючих, готової продукції, але і дозволяють проводити маркетингові дослідження для прогнозу попиту на різні види продукції, знаходити нових партнерів і багато іншого.

При цьому всі бухгалтерські операції на підприємствах і не тільки, зараз грунтуються на застосуванні інформаційних технологій. Як відомо ефективність роботи державного управління багато в чому залежить від рівня взаємодії між громадянами, підприємствами та іншими органами управління. Тому в державному управлінні інформаційні технології дозволяють одночасно використовувати інформаційні, організаційні, правові, соціально-психологічні, кадрові та інші фактори, що значно полегшує роботу і організацію самого процесу керування. Звичайно, застосування таких технологій не вирішує всіх проблем, але значно прискорюють роботу на складних ділянках аналітичної діяльності, наприклад, під час проведення аналізу та оцінки оперативної обстановки в складних ситуаціях, підготовки і формування звітів та довідок.

Застосування інформаційних технологій у науковій сфері та у сфері освіти складно переоцінити. Зараз важко уявити собі школу, в якій би не було комп'ютерного класу. Зараз існує маса електронних бібліотек, скористатися якими можна не виходячи з дому, що значно полегшує процес навчання і самоосвіти. При цьому інформаційні технології сприяють розвитку наукових знань.

Тому що збільшується швидкість обміну інформацією і з'являється можливість проводити складні математичні розрахунки за кілька секунд і багато іншого. Інформаційні технології це один із сучасних способів спілкування, головними перевагами якого є загальнодоступність. Використовуючи інформаційні технології можна з легкістю отримати доступ до цікавить вас інформації, а також поспілкуватися з живою людиною. З одного боку це має негативний ефект, оскільки люди все менше спілкуються "вживу", при безпосередньому контакті, але з іншого боку дозволять спілкуватися з людиною, яка знаходиться на іншому кінці світу, а це погодьтеся, має величезне значення.

Підвівши підсумок можна сказати, що інформаційні технології глибоко проникли в наше життя і сучасне суспільство, яке не зможе в нинішньому вигляді існувати без них.

Література:

1. http://ukrarticles.pp.ua/pk-internet/6918-znachenie-informacionnyx-texnologij-v-sovremennom-obshhestve.html

Водько Андрій Романович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ПОНЯТТЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Вступ

Світ стає все ближче до становлення інформаційного суспільства. Інформаційне суспільство - це нова і більш досконала форма соціальної організацією котра повинна допомагати всім людям в повній мірі реалізувати свій потенціал, сприяти сталому економічному та соціальному розвитку, підвищенню якості життя, скорочення рівня бідності та ліквідації голоду. У деяких країнах світу більшість переваг інформаційного суспільства стало реальністю вже сьогодні. Перш за все, це країни Західної Європи, США, Японія. Комп'ютерні технології займають найбільш важливу частину в сучасному житті суспільства. І найстрашнішою бідою для людства було б втратити всі комп'ютери одночасно. За останніми підрахунками вчених, в разі глобальної катастрофи, сільське господарство і промисловість вдасться відновити приблизно за століття. Тоді як вихід з ладу всієї обчислювальної техніки, відкине людство на три-чотири століття тому.

Поняття інформаційних технологій

Визначення інформаційних технологій

Сьогодні, в століття інформатизації і комп'ютеризації інформація є таким ж ресурсом, як трудові, матеріальні та енергетичні. Інформаційні технології - це

процеси, що використовують сукупність засобів і методів збору, обробки і передачі даних (первинної інформації) для отримання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту). Інформаційна технологія є процесом, що складається з чітко регламентованих правил виконання операцій, дій, етапів різного ступеня складності над даними, що зберігаються в комп'ютерах. Згідно з визначенням, прийнятим ЮНЕСКО, інформаційні технології - це комплекс взаємопов'язаних, наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і зберіганням інформації; обчислювальну техніку і методи організації і взаємодії з людьми і виробничим обладнанням, їх практичне використання, а також пов'язані з усім цим культурні проблеми.

Етапи розвитку інформаційних технологій:

Існує кілька точок зору на розвиток інформаційних технологій з використанням комп'ютерів, що визначаються різноманітними ознаками ділення. Загальним для всіх викладених нижче підходів є те, що з появою персонального комп'ютера почався новий етап розвитку інформаційної технології. Основною метою стає задоволення персональних інформаційних потреб людини як для професійної сфери, так і для побутової.

Ознака поділу - вид задач і процесів обробки інформації

- 1-й етап (1960-1970-ті рр.) - Опрацювання даних в обчислювальних центрах у режимі колективного користування. Основним напрямком розвитку інформаційних технологій була автоматизація операційних рутинних дій людини.
- 2-й етап (з 1980-х рр.) - Створення інформаційних технологій, спрямованих на вирішення стратегічних завдань.

Ознака поділу - проблеми, які стоять на шляху інформатизації суспільства.

- 1-й етап (до кінця 1960-х рр.) Характеризується проблемою опрацювання великих обсягів даних в умовах обмежених можливостей апаратних засобів.
- 2-й етап (до кінця 1970-х рр.) Пов'язаний з поширенням ЕОМ серії IBM / 360.
- 3-й етап (з початку 1980-х рр.) - Комп'ютер стає інструментом непрофесійного користувача, а інформаційні системи – засобом підтримки прийняття його рішень.
- 4-й етап (з початку 1990-х рр.) - Створення сучасної технології міжустановних зв'язків та інформаційних систем.

Ознака поділу - перевага, яку надає комп'ютерна технологія.

- 1-й етап (з початку 60-х рр.) Характеризується досить ефективним опрацюванням інформації при виконанні рутинних операцій з орієнтацією на централізоване колективне використання ресурсів

обчислювальних центрів. Основним критерієм оцінки ефективності інформаційних систем була різниця між витраченими на розробку і зекономленими в результаті впровадження засобами.

- 2-й етап (з середини 70-х рр.) Пов'язаний з появою персональних комп'ютерів. Змінився підхід до створення інформаційних систем - орієнтація зміщується в сторону індивідуального користувача для підтримки прийнятих ним рішень. На цьому етапі використовується як централізоване опрацювання даних, характерне для першого етапу, так і децентралізоване, що базується на розв'язанні локальних задач і роботі з локальними базами даних на робочому місці користувача.
- 3-й етап (з початку 90-х рр.) Пов'язаний з поняттям аналізу стратегічних переваг у бізнесі і заснований на досягненнях телекомунікаційної технології розподіленої обробки інформації. Відповідні інформаційні технології повинні допомогти організації вистояти в конкурентній боротьбі і отримати перевагу.

Ознака поділу - види інструментарію технології.

- 1-й етап (до другої половини XIX ст.) - "Ручна" інформаційна технологія, інструментарій якої складали: перо, чорнильниця, книга. Основна ціль технології - представлення інформації в потрібній формі.
- 2-й етап (з кінця XIX в.) - "Механічна" технологія, інструментарій якої складали: друкарська машинка, телефон, диктофон, пошта.

Основною метою інформаційних технологій -представлення інформації в потрібній формі більш зручними засобами.

- 3-й етап (40-60-ті рр. XX ст.) - "Електрична" технологія, інструментарій якої становили: великі ЕОМ і відповідне програмне забезпечення, електричні друкарські машинки, ксерокси, портативні диктофони. акцент в інформаційної технології починає переміщатися з форми представлення інформації на формування її змісту.
- 4-й етап (з початку 70-х рр.) - "Електронна" технологія, основним інструментарієм якої стають великі ЕОМ і створені на їхній базі автоматизовані системи управління та інформаційно-пошукові системи. Центр ваги технології ще більш зміщується на формування змістовної сторони інформації для управлінського середовища різних сфер суспільного життя, особливо на організацію аналітичної роботи.
- 5-й етап (з середини 80-х рр.) - "Комп'ютерна" технологія, основним інструментарієм якої є персональний комп'ютер із широким спектром стандартних програмних продуктів різного призначення. У зв'язку з переходом на мікропроцесорну базу суттєвим змінам піддаються і технічні засоби побутового, культурного та інших призначень. Починають широко використовуватися в різноманітних галузях глобальні і локальні комп'ютерні мережі.

Значення інформаційних технологій в житті сучасної людини

Ніхто не стане заперечувати величезне значення, яке мають інформаційні технології в життя звичайної людини, навряд чи хто-небудь зможе назвати сферу, де вони не використовуються хоча б побічно. Починаючи від вузько спеціалізованих областей важкої промисловості і закінчуючи такими речами, як обробка фотографій - всюди інформаційні технології прямо або побічно, знаходять своє застосування. Будь-які бухгалтерські операції на будь-якому підприємстві сьогодні проводяться з використанням комп'ютера. Те, наскільки ефективно працює міське самоврядування, багато в чому визначається тими технічними засобами і тим програмним забезпеченням, які в неї є. Природно, використання найостанніших технологій і технічних засобів не вирішує повністю всіх проблем, проте інновації можуть значно спростити і прискорити роботу службовців. Особливо це помітно на складних ділянках аналітичної діяльності, в процесах формування звітів і довідок. На особливу увагу заслуговують технології, використовувані в сфері освіти, їх значення важко переоцінити. Дуже складно знайти школу, в якій не було б комп'ютерного класу. А Інтернет надає школяреві масу інформації, отримати яку можна за кілька хвилин. Таким чином, інформаційні технології можуть значно полегшити процес освіти і навчання. Швидкість передачі інформації зростає щодня, зростають і технологічні потужності. За допомогою технічних засобів люди з різних кінців Землі можуть
спілкуватися один з одним, Інтернет - це один з найпопулярніших способів зв'язку на сьогоднішній день, головним чином тому, що він є загальнодоступним. Також інформаційні технології сьогодні дозволяють людям практично миттєво отримати доступ до необхідної інформації. ІТ в різних сферах діяльності людини: промисловість, транспорт, сільське господарство, індустрія відпочинку і розваг - все безпосередньо залежить від комп'ютерів. Кількість галузей, в яких задіяні цифрові технології неухильно зростає. Потрібно все більше фахівців для їх обслуговування. Поступово відходить у минуле важка людська праця. З'являються нові спеціальності та професії . Сьогодні по оцінкам експертів 90% всіх транспортних переміщень людей пов'язане з інформаційними цілями (наради, підписи, довідки і т.д.). Особливий внесок ІТ внесли в сферу освіти, де були повністю комп'ютеризовано всі навчальні заклади, що дозволяло в значній мірі полегшити процес навчання і освіти. Простий приклад того наскільки ми залежимо від комп'ютерів - автомобіль. Сьогодні при відмові або збої в електричної складової, машина просто не зможе зрушити з місця. Високі технології проникли і захопили всі сфери суспільного життя. Інтернет і соціальні мережі: життя безпосередньо залежить від комп'ютера та Інтернету. Також інформаційні технології сьогодні дозволяють людям практично миттєво отримати доступ до необхідної інформації. Небезпека комп'ютерних технологій: вплив на психіку людини. Залежність виражається в двох основних формах: інтернет-залежність і надмірна захопленість комп'ютерними іграми. Ми не будемо заглиблюватися в суть цих проблем, адже при грамотному використанні комп'ютерних технологій

користі незрівнянно більше, і ми це відчуваємо з кожним днем все більше і більше.

Висновок

Підводячи підсумок, можна сказати, що інформаційні технології дуже глибоко проникли в життя сучасної людини, і навіть більше того – без інформаційних технологій сучасне суспільство не зможе існувати в тому вигляді, в якому воно знаходиться зараз. В даній роботі розглядається історія розвитку інформаційних технологій. Вона включає в себе залежно від ознаки поділу від двох до п'яти етапів. За першою ознакою ділення розглядається 2 етапи зміни виду завдань і процесів обробки інформації. За другим - 4 етапи виникнення та вирішення проблем, що стоять на шляху інформатизації суспільства. По третьому - 3 етапу формування переваг комп'ютерних технологій. І по четвертому - 5 етапів зміни видів інструментарію технології. Крім того, в роботі було визначено значення інформаційних технологій для сучасної людини. Інформаційні технології використовуються в усіх сферах діяльності людини: починаючи від вузькоспеціалізованих областей важкої промисловості і закінчуючи обробкою фотографій; і що найголовніше, вони дозволяють практично миттєво отримати доступ до необхідної інформації. А обмін інформацією здійснюється за допомогою засобів радіоелектроніки. Таким чином, в процесі роботи ми зробили акцент на використанні сучасних технологій для інформаційного забезпечення всіх сфер діяльності людини, так як останнім часом вони набувають дуже важливе значення.

Література:

1) Інформаційні ресурси і документальні бази даних: Навч. посібник / О.М. Васіна, О.Л. Голіцина, Н.В. Максимов, І.І. Попов.
2) Попов І.І. Інформаційні ресурси і системи: реалізація, моделювання, управління.
3) Попов І.І., Храмцов П.Б., Максимов Н.В. Введення в мережеві інформаційні ресурси та технології.
4) https://uk.wikipedia.org/wiki/Інформаційні_технології

Примаченко В.І., аспірант,
Державний університет телекомунікацій,
Факультет Інформаційних технологій

м. Київ

АЛГОРИТМ ВИКОНАННЯ ОПЕРАЦІЙ OFDM-МОДУЛЯЦІЇ В SDR

The paper shows the architecture of telecommunication equipment constructed on the basis of software-driven systems. The functional circuit that ensures the implementation of the basic requirements of SDR. Determined that the program operated radio, could be realized many years ago. However, due to lack of sufficiently powerful development capabilities of DSPs and programmable logic integrated circuits have become widespread SDR in just this decade. It is shown that a digital signal processor or microprocessor must have a high level of computing power. The development of components already allows you to create a system SDR, and in conjunction with software and control system - the network of the future. Determined that systems for high speed data transmission of broadband signals associated with problems for the recipient, through the formation of additional channels caused by inter-symbol noise (inter-symbol interference). To effectively eliminate inter-symbol interference and reduce complexity equalizer technology is OFDM. The basic idea of OFDM technology is to divide the frequency-selective channel into a number of narrowband subchannels. For these subchannels or subcarriers orthogonal narrowband signals are transmitted in parallel. As each of these signals is experiencing shallow fading, it is very simple correction scalar channel. The algorithm operations OFDM-modulation to SDR.

Історично склалося, що нові покоління технологій радіодоступу впроваджуються з інтервалом приблизно десять років, щоб впоратися з ростом мобільного Інтернет-трафіка. Це дозволяє в повній мірі скористатися еволюцією технологічні компоненти без яких-небудь застарілого тягаря.

В 2010 р. завершено розробку специфікацій технології Long Term Evolution - Advanced (LTE-A), яка відноситься до 4-го покоління (4G) технологій мобільного зв'язку. Технології радіодоступу 5-го покоління (5G), як очікується, стануть доступні для комерційного запуску близько 2020 р. [1, с. 1]. Їх розвиток триватиме до 2030, після чого ми зможемо отримати потенційний досвід користування технологіями 6-го покоління (6G).

Варто відзначити, що базовою технологією модуляції так і залишається технологія OFDM. Після перетворення паралельного коду в послідовний часовий інтервал OFDM-сигналу має форму

(1)

для $n = 0...M-1$. Як видно, це тільки сума складних експоненціалів, тобто синусоїдальні і косинусоїдальні функції [2, с. 3; 3, с. 1].

Виходячи з вищесказаного на рис. 1 представлено алгоритм виконання операцій OFDM-модуляції. Перший блок в алгоритмі відповідає за введення вхідних даних та визначення характеристик операндів які будуть використовуватись в подальших розрахунках.

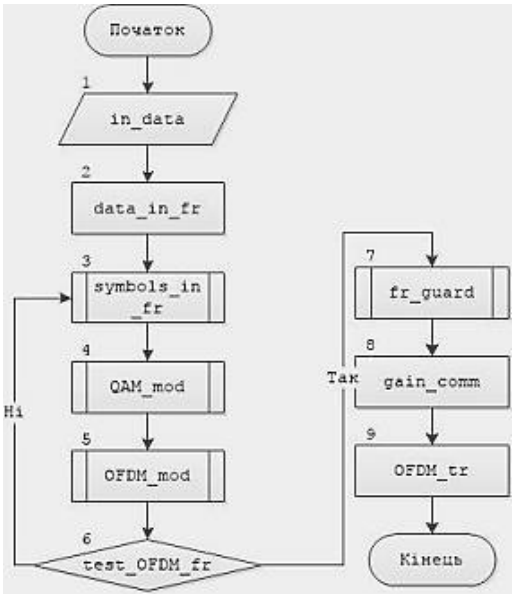


Рис. 1. Алгоритм виконання операцій OFDM-модуляції

В наступному блоці виконуються операції формування потоку даних в кадри. Блок номер 3 визначає кількість символів на кадр. В блоках 4 та 5 виконуються операції QAM-модуляції (або іншого виду модуляції в залежності з потребою) та OFDM-модуляція за допомогою ОШПФ. Перевірка сформованості OFDM-кадру виконується в 6 циклічному блоці. Наступний блок призначений для визначення, формування та додавання до OFDM-кадру захисного інтервалу. Операція підсилення амплітудного значення кадру відповідно до рівня каналу зв'язку виконується в 8 блоці. Останній блок виконує функцію попередньої підготовки до формування вихідного сигналу, можливість виведення даних і підключення ЦАП.

В статті виконано опис роботи розробленого алгоритму виконання операцій OFDM-модуляції. Перевагою даного алгоритму є можливість його реалізації в SDR.

Література

1. Mogensen Preben, Pajukoski Kari, Tiirola E. 5G small cell optimized radio design [Електронний ресурс] Preben Mogensen, Kari Pajukoski, E. Tiirola // – Режим доступу: https://www.researchgate.net/publication/ 269304509_5G_small_cell_optimized_radio_design

2. Hammarberg P., Rusek F., Salvo Rossi P., and Edfors O. EXIT Chart Evaluation of a Receiver Structure for Multi-User Multi-Antenna OFDM Systems [Електронний ресурс] P. Hammarberg, F. Rusek, P. Salvo Rossi, O. Edfors // – Режим доступу: http://tlc.dii.unina2.it/tlc/files/publications /2009%20IEEE%20globecom%202.pdf

3. Munier Florent, Eriksson Thomas, Svensson Arne Receiver algorithms for OFDM systems in phase noise and AWGN [Електронний ресурс] Florent Munier, Thomas Eriksson, Arne Svensson // – Режим доступу: https://www.researchgate.net/publication/2906843_Receiver_algorithms_for_ OFDM_ systems _ in_ phase_noise_and_AWGN

Якубенко Ірина Миколаївна,
Державний університет телекомунікацій,

Навчально-науковий інститут
менеджменту та підприємництва,
кафедра менеджменту, аспірант
м. Київ

ОБҐРУНТУВАННЯ ОРІЄНТИРІВ КОМУНІКАЦІЙНОЇ ПОЛІТИКИ ПІДПРИЄМСТВА

Управління комунікаційною політикою в сучасних умовах вийшло на новий рівень - постійне підвищення ролі інформації в діяльності організації змушує її переглядати свої позиції, зокрема в сфері комунікацій. Застосування комунікацій у системі управління підприємством передбачає наявність єдиної системи планування комунікаційної політики підприємства. Великого значення за останній час набуває інтеграція різних елементів комунікаційної політики в єдине ціле.

Світ змінюється. З переходом в епоху інформаційної цивілізації та побудови новітніх технологій управління все розвивається та постійно вдосконалюється. Інформацію в управлінні можна назвати сигналом/повідомлення про будь-яку можливу/реальну подію, яка відбулася в організації.

Комунікація є системною роботою. Вона потребує планування, базованого на дослідженнях, і повинна охоплювати весь спектр можливих форматів та каналів.

Науковці по різному тлумачать зміст комунікації. У широкому значенні – це різновид взаємодії між тими чи іншими суб'єктами інформаційного впливу за посередництвом певного визначеного об'єкта, тобто повідомлення. Отже, мова йде про взаємодію певних людей, груп людей, соціальних інститутів, суспільства загалом. Український дослідник В. Бебик пропонує таке визначення поняття комунікації: «Комунікація — це опосередкована і цілеспрямована взаємодія двох суб'єктів, яка може відбутися як в реальному, так і віртуальному просторі і часі». Будь-яка комунікація передбачає передачу інформації, тому визначає відносини і, як наслідок, взаємовідносини між суб'єктами, які перебувають у процесі комунікації.

В організації одним з найбільш важливих важелів управління є комунікаційна політика. Комунікаційна політика підприємства представляє собою інструмент впливу підприємства на зовнішню і внутрішню середу за допомогою інформаційної взаємодії. Її розуміють, як процес формування спрямованих на ринок і від ринку (при ринкових дослідженнях) потоків інформації.

Теоретичним і практичним аспектам комунікацій, проблемам удосконалення здійснення процесу управління комунікацій присвячено багато наукових досліджень. Вагомий внесок в дослідження комунікаційної політики, та, зокрема, проблеми управління комунікаційною політикою підприємства в сучасних умовах, зробили такі вітчизняні та зарубіжні науковці й фахівці, як Р. Джозлін, Ф. Котлер, С. Гаркавенко, Л. Балабанова, О. Громова, В. Шепель, П.

Мацкевич, П. Роуз, М. Ковальов та інші, проте питання щодо ефективних методів управління комунікаційною політикою потребують більш глибшого дослідження [2, с.53].

Комунікаційна політика підприємства обмежена вузьким ринковим сегментом корпоративної клієнтури, яку вони, якщо і збільшують, то за допомогою засобів прямого маркетингу і реклами. Комунікаційна політика зосереджується не лише на великій корпоративній клієнтурі, а й на етапі проникнення на ринок активно використовується такий інструмент комунікаційної політики, як лобіювання.

Належний рівень організації комунікацій має спрямовуватись на вирішення низки питань з розвитку та обґрунтуванню певних орієнтирів комунікаційної політики підприємства з урахуванням позицій всіх зацікавлених сторін.

Орієнтири комунікаційної політики базуються на трьох основних компонентах:

1. Мотиваційному – бажанні спільно працювати, творити, реалізовувати поставлені цілі.

2. Змістовному – розумінні, як спільно працювати, спілкуватися задля досягнення тієї чи іншої мети.

3. Операційному – готовності до спільної діяльності (наявності для цього необхідних знань, умінь, навичок).

Ефективна комунікація з точки зору відправника передбачає отримання інформації одержувачем і реакцію у відповідь згідно з прогнозом відправника. Для підвищення ефективності всієї системи комунікації необхідно зменшити перешкоди, що виникають у процесі комунікації, тобто враховувати індивідуально-особистісні, соціальні і культурні фільтри. Ці перешкоди можуть бути змінені за рахунок дублювання повідомлення, зміни самого повідомлення у разі необхідності, зменшення числа посередників у комунікативному процесі [3, с.211].

Комунікативну взаємодію між центрами прийняття управлінських рішень можна розглядати як інформування, взаємовплив, певні взаємовідносини між її учасниками для досягнення порозуміння.

Обґрунтування орієнтирів комунікаційної політики базується на основних засадах менеджменту:

- планування і управління комунікативними процесами, в т.ч. виявлення цільових аудиторій, розробку комунікаційних стратегій, контроль та оцінку ефективності комунікацій;

- роз'яснення позицій і напрямків підприємства та конкретної персони;

- організацію інформаційного трансферту (перенесення, переклад) і діалогу;

- інформаційне представлення інтересів об'єкта;

- формування і посилення довіри та симпатії;

- уявлення того чи іншого об'єкта (організації, персони, проблеми, теми) громадськості та збільшення компетентності учасників діалогу;

- твердження коректних комунікацій в конфліктних ситуаціях.

Для комунікаційної політики підприємства важливим є інтенсивне ділове спілкування з партнерами, потенційними клієнтами і постачальниками, що забезпечують обмін інформацією на певних етапах проходження цієї інформації.

Визначення комунікаційних мереж керівниками особливо важливе для розуміння влади, мотивації і контролю в системі підприємства, бо покриття або централізація інформації підтримують владні відносини, а характер взаємозалежності функцій, підфункцій працівників на підприємстві визначає тип більш ефективної комунікаційної мережі. Добре налагоджені комунікаційні орієнтири створюють позитивний соціально-психологічний клімат підприємств.

Література:

1.Любченко Н.Л. Система комунікаційного менеджменту підприємства / Н.Л. Любченко // Науковий виробничий журнал «Інноваційна економіка». – 2013. – № 48. – С. 40-45.

2 . Примак Т. О. Маркетингові комунікації в системі управління підприємством. — К.: Експерт, 2010. – 383с.

3. Шпак Н. О. Основи комунікаційного менеджменту промислових підприємств: монографія / Н. О. Шпак. – Львів: Видавництво Львівської політехніки, 2011. – 328 с.

Шигида Богдан Андрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

ВАЖЛИВІСТЬ ВИВЧЕННЯ ІНФОРМАТИКИ І ОНОВ ПРОГРАМУВАННЯ ДЛЯ РОЗВИТКУ СТУДЕНТІВ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Розвиток інформаційного суспільства зумовлює потребу у нових підходах до навчання інформатики учнів вищих навчальних закладів.

Курс інформатики набуває нового функціонального призначення, спрямованого на формування інформаційної культури, інформаційної компетентності, усвідомлення учнями ролі інформаційних технологій у розвитку сучасного суспільства.

На даному етапі становлення і розвиток нової наукової дисципліни, здатної формулювати і вивчати основні закономірності процесу інформатизації сучасного світу, є об'єктивною і настійною необхідністю. Інформатика виникла в рамках сучасних теорій управління складними динамічними процесами і була покликана додати теоріям практичної спрямованості, зорієнтованої на створення наукових основ функціонування складних інформаційних систем, що

ґрунтуються на широкому використанні новітніх технологій інформаційного обміну.

Розвиток інформаційних технологій відбувається настільки швидко, що традиційне «навчання на все життя», тобто формування знань, умінь і навичок, яких раніше було достатньо людині для виконання суспільно значущої діяльності протягом багатьох років,нині неможливе. Більше того, перманентне оновлення змісту навчання інформатики в темпі, який би забезпечував, принаймні, оволодіння учнем засобами діяльності, які існують на момент його навчання,теж неможливе з низки причин. Отже, цілепокладання навчання інформатики має відповідати досить суперечливим вимогам: забезпечити освоєння учнем певних видів і засобів діяльності й створити передумови самостійного освоєння ним засобів діяльності, яких на момент навчання не існувало. Виходячи з принципів дидактики (науковості і доступності, послідовності викладання і міцності знань тощо), можна запропонувати подолання суперечностей шляхом поєднання навчання в діяльності з фундаменталізацією набутих знань. Це стає можливим, якщо сформулювати проміжні цілі етапів навчання й апарат визначення рівня навчальних досягнень так, щоб забезпечити не формальне засвоєння прийомів діяльності, а засвоєння прийомів пошуку шляхів розв’язування простих загальноінформатичних задач і об’єднання їх у розв’язані прикладної задачі мовного і графічного обміну інформацією.

Під час навчання в студентів має бути сформовано як теоретична база знань з основ інформатики, так і вміння й навички ефективного використання ними сучасних комп'ютерно-інформаційних технологій у навчально-пізнавальній та майбутній професійній діяльності. Створення і широке використання в повсякденному житті сучасного суспільства новітніх технологій збирання та обробки інформації, різних інформаційно-пошукових, моделюючих, аналітичних і управлінських систем обумовили виникнення цікавого і значного феномена, характерного для новітньої історії людства. Вдосконалення засобів обчислювальної техніки, систем телекомунікацій та інформаційних технологій не лише повною мірою виявляє свою виробничу, технологічну й соціальну корисність, поліпшуючи умови нашої праці і побуту, вони радикальним чином змінюють саму природу людських і виробничих відносин у сучасному суспільстві.

Важливою особливістю інформатики є те, що вона має найширші застосування, що охоплюють, в основному, всі види людської діяльності виробництво, управління, науку, освіту, проектні розробки, торгівлю, грошово-касові операції, медицину, криміналістику, охорону навколишньою середовища, мистецтвознавство, побут тощо Основне значення має вдосконалення соціального управління на основі нових інформаційно-переробних технологій Інформатика вивчає те спільне, що властиве численним різновидам конкретних інформаційних процесів (технологій) Ці технології і є об'єктом вивчення інформатики.

Мета, зміст, форми й методи навчання інформатики вибудовуються на основі парадигми центризму, єдності навчання, виховання і розвитку особистості як методології освіти, яка ґрунтується на гуманістичних цінностях. Вимоги до загальноосвітньої підготовки студентів з інформатики розробляються на засадах компетентнісного і особистісно зорієнтованого підходів, відповідно до яких кінцевим результатом навчання є предметна інформатична компетентністю, ключові компетентності, зокрема: уміння вчитися, математична і базові компетентності в галузі природознавства і техніки, інформаційно комунікаційна, комунікативна, соціальна, громадянська. Зазначені компетентності базуються на набутих суб'єктом навчання знаннях, уміннях і навичках, його досвіді навчальної й життєвої діяльності, вироблених ціннісних орієнтаціях, позитивній мотивації.

Отже, досягатиметься соціально зумовлена мета навчання інформатики у системі загальної освіти — задоволення потреб суспільства у особистостях, здатних використовувати досягнення інформаційно-комунікаційних технологій у повсякденному житті, продуктивній діяльності

Література:

1. http://ukped.com/skarbnichka/322-.html
2. https://sites.google.com/site/informatikavpocatkovihk/
3. http://uabs.edu.ua/images/stories/docs/K_VM/Holovan_06.pdf
4. http://klasnaocinka.com.ua/uk/article/informatika-v-zhitti-suspilstva.html
5. http://uabs.edu.ua/images/stories/docs/K_VM/Holovan_06.pdf

Колісніченко І.Ю., *студент*
Житомирсткий державний технологічний університет
м. Житомир

ПРОЕКТУВАННЯ СИСТЕМИ АВТОМАТИЗАЦІЇ РОБОТИ БІБЛІОТЕКИ

Із кожним днем все більше і більше підприємств автоматизуються. Серед таких є і бібліотеки. На жаль їх автоматизація обмежена базовим функціоналом і не націлена на їх відвідувачів. Дана робота дозволить розширити базовий функціонал і покращити взаємодію з відвідувачем.

Для удосконалення роботи бібліотеки було проаналізовано її роботу та вивчено слабкі сторони. Серед них було виділено такі як рукописна частина, запис історії, оформлення документів на книги. Після цього виникла задача їх автоматизувати та додати функціонал для покращення взаємодії бібліотеки і користувача.

Спроектована система призначена для автоматизації бібліотеки, гнучкого відстеження та аналізу книг, для інформації користувачам. Вона полягає у

зчитуванні штрих кодів, занесення та зберігання в базу даних інформацію, що містить в собі назви книжок, авторів, особисту інформацію відвідувача, історію користування книжками та синхронізацією з мобільним додатком, який надасть можливість відвідувачам “перебувати” у бібліотеці віддалено.

Метою створення даної системи було удосконалити роботу працівникам і надати більше інформації відвідувачам. Крім цього клієнти отримають можливість переглянути список книг у своєму додатку на телефоні, також могли бачити рейтинг книги, який складався відвідувачами цієї бібліотеки, могли прочитати рецензію для визначення більш підходящої книги та залишити свій відгук. Система буде сповіщати про надходження нових книжок, клієнти будуть бачити книги, які мають згодом з’явитись в бібліотеці. Обмін інформацією між бібліотекою та мобільним додатком відбувається завдяки мобільній мережі інтернет.

Розвиток мобільного інтернету надає можливість відвідувачам постійно синхронізувати дані, тобто всі зміни в бібілотеці вони отримають моментально у своєму додатку.

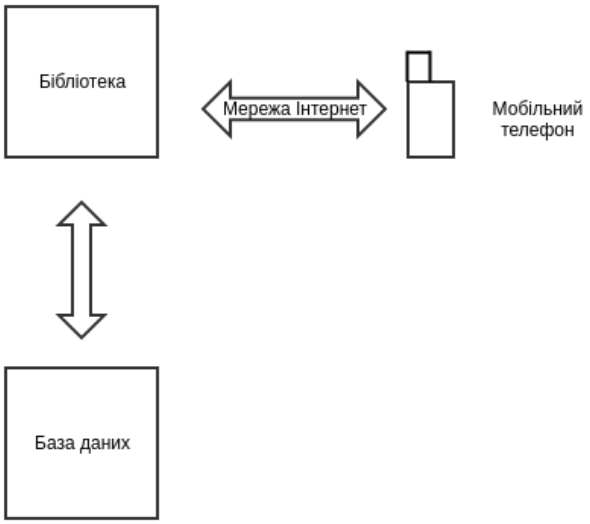


Рис. 1. Схема взаємодії елементів системи

На рис. 1 представлена схема, на якій показано автоматизовану систему бібліотекм. Бібліотека - це система для обробки, редагувати та зберігати інформацію. Відвідувачі зможуть отримати всю цю інформацію на свій власний телефон через мережу Інтернет. В них буде можливість прочитати рецензію на обрану книгу, побачити її рейтинг, забронювати її, переглянути відгуки інших користувачів, додати свій відгук, переконатись в наявності книжок. Вся інформація зберігається в базі даних, яка може знаходитись як на тому ж сервері, що і програмне забезпечення, так і на віддаленому.

Література

1. Анализ и проектирование информационных систем с помощью UML 2.0, 2016.

2. Software Requirements 2, March, 26, 2003.

3. Проектирование информационных систем, 2008.

Коник Р.С.,
аспірант кафедри Інженерії програмного забезпечення,
Державний університет телекомунікацій,
м. Київ

АНАЛІЗ МЕТОДИКИ ПІДВИЩЕННЯ ЖИВУЧОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

У «глобальному суспільстві ризику» виникають нові вимоги до безпеки технічних систем, які включені у ланцюги життєзабезпечення, пов'язані безпосередньо з повсякденною діяльністю людей. Уже на початковому етапі розробки та впровадження цих систем потрібно якомога правильніше визначитися з цілями й необхідним рівнем безпеки, спрогнозувати можливі втрати у разі виникнення нештатних ситуацій, мати можливість попереджувати розвиток небезпечних станів системи, спланувати способи відновлення функціонування або «безпечну зупинку».

Сучасні дослідження з теорії живучості складних технічних систем спрямовані саме на розвиток методологічних основ організації систем із підвищеним рівнем живучості та безпеки упродовж всього життєвого циклу; на вивчення закономірностей збереження системою певної якості при ушкодженні її елементів і способах забезпечення живучості, використання механізмів її підтримки.

У теорії живучості термін «якість системи» розуміється як властивість здатності досягати цілі функціонування (реалізовувати визначену функцію). Аналогічно у теорії надійності якість системи розуміється лише у властивості гарантувати працездатний стан чи ні.

Ушкодження компонентів — це подія, що призводить до порушення функціонування системи або її складових внаслідок зовнішніх чи внутрішніх впливів. Важлива не природа впливів, а їхні наслідки для системи. Ушкодження можуть бути суттєвими або несуттєвими. Суттєві ушкодження найчастіше призводять до зміни цілі функціонування системи (звужується множина функцій, які виконуються системою), несуттєві — не призводять до зміни цілі.

Живучість — властивість, що характеризує, зокрема, і здатність системи ефективно функціонувати за наявності ушкоджень (руйнацій складових) або відновлювати цю здатність за визначений проміжок часу.

Живучість є комплексною властивістю систем. Показники живучості мають відповідати вимогам системного рівня досліджень і в той же час вони мають забезпечити можливість розробки достатньо простих моделей для практичних робочих досліджень та виконання розрахунків. З поняттям живучості тісно пов'язані також такі властивості системи як адаптивність та стійкість. Адаптивність — це здатність системи змінюватися при зміні умов функціонування заради збереження своїх експлуатаційних показників у визначених межах. Стійкість — властивість системи при незначних змінах умов функціонування зберігати свої експлуатаційні показники.

Для технічних систем зі складною архітектурою, з великою кількістю гетерогенних компонентів оцінити живучість є складним завданням, навіть якщо відомі необхідні метрики для всіх складових системи, проте існує нагальна потреба у простих і достатньо ефективних для практики методиках адекватної достовірної оцінки основних характеристик живучості. Зрозуміло, що при дослідженні живучості та побудові оцінок необхідно провести аналіз інтегральних багатофакторних (багатокритеріальних) показників, які враховують як кількісні, так і якісні характеристики.

Сучасні дослідження живучості складних технічних систем спираються на принципи системного аналізу, що забезпечує формування цілісного системного погляду на об'єкт аналізу і дозволяє врахувати наступні особливості, які, згідно із загальною теорією систем, притаманні складним системам:

— вкладеність — значна кількість зв'язаних і взаємодіючих між собою складових

системи, які в свою чергу складаються з великої кількості зв'язаних і взаємодіючих між собою складових (елементів, підсистем, компонентів) і т.д.;

— наявність загальносистемної цілі функціонування, яка домінує над цілями функціонування будь-яких складових системи;

— непередбачуваність, що виявляється у поведінці складної системи, яка є результатом взаємодії і взаємовідношень між її компонентами;

— відсутність повної інформації про систему в цілому у будь-якого з компонентів складної системи, оскільки зв'язки між компонентами досить короткі, інформацію елемент системи отримує від найближчих сусідів, а при передачі на відносно великі відстані (при передачі інформації через певну кількість елементів) вона зазнає змін (а іноді взагалі втрачається);

— нелінійність відношень між компонентами, внаслідок чого незначний збурюючий вплив може викликати помітний ефект, і навпаки, значний впливаючий імпульс може бути не результативним;

— наявність зворотних зв'язків як позитивних, так і негативних, що визначають функціонування системи;

— відкритість (межі системи залежно від її природи мають бути проникні або для інформації, або для енергії, через що система постійно змінюється, але засобами управління утримується в стабільному стані);

— наявність історії, причому незначні зміни в теперішньому можуть призвести до значних змін у майбутньому;

— активна взаємодія із зовнішнім середовищем в умовах невизначеності факторів впливу на складові системи і мінливості стану зовнішнього і внутрішнього середовищ.

Література:

1. Додонов А.Г., Ландэ Д.В. Живучесть информационных систем. – К.: Наук. думка, 2011. – 256 с.

2. Громов Ю.Ю., Драчев В.О., Набатов К.А., Иванова О.Г. Синтез и анализ живучести сетевых систем: монограф. – М.: Изд-во Машиностроение-1, 2007. – 152 с.

3. Додонов О.Г. Інформаційні потоки в глобальних комп'ютерних мережах. – К.: Наук. думка, 2009. – 295 с.

4. Князева Н.А., Ненов А.Л. Метод оценки структурной надежности сети при изменении ее структуры. – К.: Вісник ДУІКТ. – Т. 9. – №4. – 2011. − С. 318-325.

Пантелемонов О.Д.

Національний авіаційний університет

м. Київ

ОПТИМАЛЬНЕ РІШЕННЯ ПРОБЛЕМ РОЗМЕЖУВАННЯ ДОСТУПУ НА ПІДПРИЄМСТВІ

У наш час контроль і розмежування доступу стали повсякденним явищем. Установка системи контролю доступу дуже швидко окупається за рахунок економії на зарплаті та зменшенні розміру збитків, пов'язаних із крадіжками як речей, так і інформації, що становить комерційну таємницю. Втрата або розголошення останньої, як правило, приводить до упущеної вигоди, розмір якої в рази може перевищувати вартість установки системи контролю доступу.

Дивлячись на неухильне зростання інтересу до СКД і перспективу широкого їх застосування в найближчому майбутньому, не слід забувати, що СКД лише спрощує процес ідентифікації, економить час і підвищує

ефективність роботи служб безпеки підприємства, але, при цьому, все одно вимагає контролю з боку людини. Відсутність досвіду в сфері використання СКД серед покупців і відсутність фахівців вищого класу, здатних здійснювати ремонт і техобслуговування на високому рівні і в стислі терміни, призводить до помилок і недоліків, допущеним в процесі проектування систем, порушень правил експлуатації, що в цілому, значно знижує ефективність і доцільність застосування СКД.

Вибір варіанта СКД нерозривно пов'язаний з вимогами до забезпечення безпеки конкретного об'єкта. При виборі систем необхідно враховувати, що можливість проведення аналітичної роботи із застосуванням сучасних програмно-апаратних комплексів СКД є необхідною якісною характеристикою системи.Ефективність використання будь-яких технічних засобів СКД залежить від застосовуваної технології контролю доступу та кваліфікації оперативно-технічного персоналу.

Система, що пропонується, для контролю і управління доступом Fortnet призначена для вирішення завдань з регулювання та моніторингу доступу людей і інших об'єктів (наприклад, автотранспорту) через обладнані точки проходу. В рамках розмежування рівнів доступу персоналу і відвідувачів та забезпечення різних рівнів безпеки в СКД Fortnet передбачені гнучкі механізми контролю переміщень об'єктів як на рівні точок проходу (картки з PIN, прохід через тамбур-шлюз, додатковий датчик проходу), так і на рівні логічного контролю дій об'єкта (напр. заборона повторного проходу).

Централізовані мережеві системи контролю доступу FortNet будуються на основі керуючого контролера ABC-E.

В якості автономного сегмента системи контролю доступу або як елемент розподіленої мережевої СКД може виступати інтегрований контролер ANC-E, що поєднує в собі аналітичні можливості керуючого контролера і можливості управління зовнішнім виконавчим обладнанням (електромагнітний замок, турнікет, шлагбаум).

Програмно-апаратний комплекс FortNet являє собою приклад гідного рішення в контексті необхідності забезпечення обмеження та розмежування доступу на об’єктах як господарської, так і інформаційної діяльності. Апаратне забезпечення в сумісності з програмним додатком, розробленим спеціально для даного обладнання дозволяють здійснювати зручний моніторинг та контроль за розмежуванням доступу на підприємствах.

Література:

1.Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.

2.Горлицин И. Контроль и управление доступом - просто и надежно КТЦ "Охранные системы", 2002.

3. Бондарчук А. П. Дослідження принципів системного підходу до проектування системи радіозв'язку //Наукові записки Українського науково-дослідного інституту зв'язку. – 2013. – №. 2. – С. 44-47.

4. http://www.intersyst.ru/solutions/165/460/

Лещук А.О., Патрікей А.В.,
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ПІДПРИЄМСТВА ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Комплексна система антивірусного захисту – це сукупність організаційних, правових та програмно-апаратних заходів і засобів, спрямованих на забезпечення ефективного антивірусного захисту інформації в локальній мережі. Комплексність системи антивірусного захисту досягається контролем всіх інформаційних потоків, що протікають в локальній мережі і узгодженням між собою різнорідних методів і засобів, що забезпечують антивірусний захист всіх елементів локальної мережі.

При організації захисту мережі потрібно брати до уваги:

Трудомісткість обслуговування
5. Відмовостійкість
6. Критичність системи
7. Людський фактор

В основу побудови комплексної системи антивірусного захисту можуть бути покладені наступні принципи:

принцип реалізації єдиної технічної політики при обґрунтуванні вибору антивірусних продуктів для різних сегментів локальної мережі;

принцип повноти охоплення системою антивірусного захисту всієї локальної мережі організації;

принцип безперервності контролю локальної мережі підприємства, для своєчасного виявлення комп'ютерної інфекції;

принцип централізованого управління антивірусним захистом;

З урахуванням цих принципів у комплексній системі інформаційної безпеки створюється підрозділ антивірусного захисту, який повинен вирішувати такі завдання:

придбання, встановлення та своєчасна заміна антивірусних пакетів на серверах і робочих станціях користувачів;
контроль правильності застосування антивірусного ПО користувачами;
виявлення вірусів в локальній мережі, їх оперативне лікування, видалення заражених об'єктів, локалізація заражених ділянок мережі;
своєчасне оповіщення користувачів про виявлених або можливих вірусів, їх ознаки та характеристики.

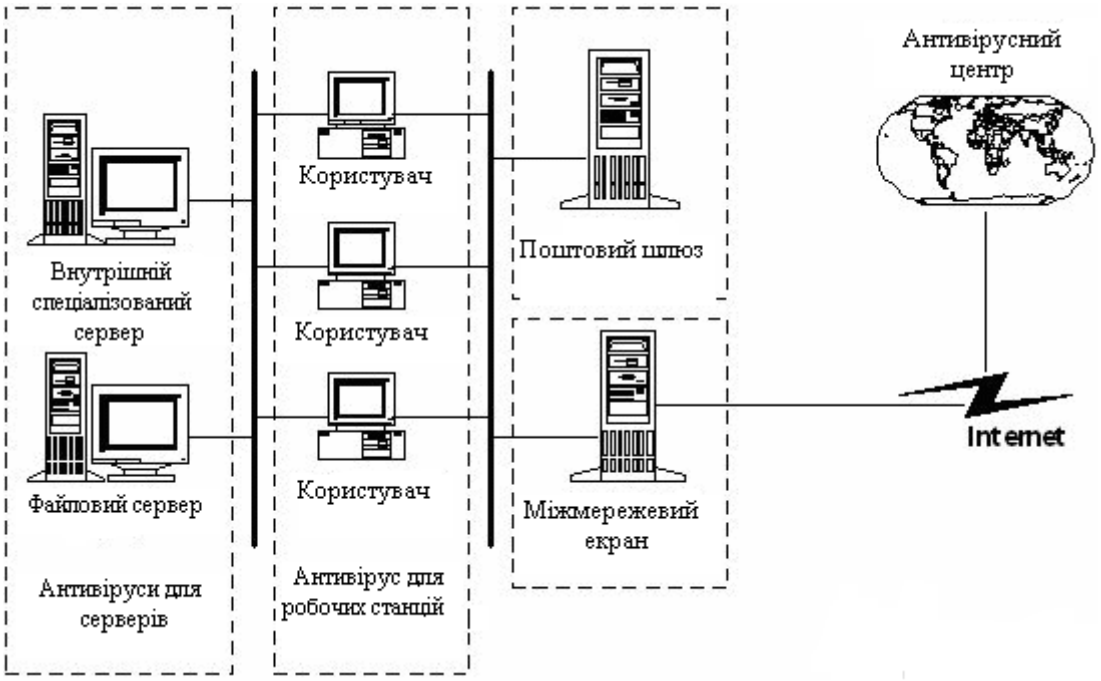
Практична реалізація антивірусного захисту інформації на серверах і ПК корпоративної мережі здійснюється з використанням низки програмно-технічних методів, які є стандартними, але мають свою специфіку, яка визначається особливостями корпоративної мережі. До них відносяться:

використання антивірусних пакетів;
архівування інформації;
резервування інформації;
ведення бази даних про віруси і їх характеристики;

Використовувані антивірусні засоби повинні відповідати таким загальним вимогам:

система повинна бути сумісна з операційними системами серверів і ПК;
система антивірусного захисту не повинна порушувати логіку роботи інших використовуваних додатків;
наявність повного набору антивірусних функцій, необхідних для забезпечення антивірусного контролю та знешкодження всіх відомих вірусів;
частота оновлення антивірусного ПЗ і гарантії постачальників (розробників) щодо її своєчасності.

При комплексному захисті локальної мережі необхідно приділити увагу всім можливим точкам проникнення вірусів в мережу ззовні.



На малюнку вище наведена загальна структура антивірусного захисту локальної мережі. На першому рівні захищають підключення в Інтернет або мережу постачальника послуг зв'язку.

Застосування антивірусів для міжмережевих екранів на сьогоднішній день зводиться до здійснення фільтрації доступу в Інтернет при одночасній перевірці на віруси трафіку. Антивірусного захисту підлягають усі компоненти інформаційної системи, що беруть участь у транспортуванні інформації та / або її зберіганні:

- файл-сервери;
- робочі станції;
- робочі станції мобільних користувачів;
- сервера резервного копіювання;
- поштові сервера.

Сучасні антивірусні пакети містять в собі наступні основні програмні компоненти: монітор, сканер, мережевий центр управління, додаткові модулі, що забезпечують перевірку електронної пошти та Web-сторінок в момент отримання інформації.

Програми "монітор" і "сканер" встановлюються як на серверах, так і на ПК, причому перший налаштовується на постійне включення.

При виявленні вірусів користувачам не рекомендується займатися "самолікуванням", так як це може призвести до втрати інформації. У таких випадках їм слід по "гарячій лінії" звертатися до адміністраторів антивірусного захисту, які вживають заходів щодо знешкодження вірусів та запобігання подальшого зараження.

Висновок: Для забезпечення захисту інформації від її знищення, компрометації чи перехвату, на підприємствах слід використовувати комплексну систему антивірусного захисту.

Перелік використаної літератури

1) *https://uk.wikipedia.org/wiki/97*
2) *http://www.rusnauka.com/13_NPN_2010/Economics/65282.doc.htm*

Мартиненко О.О.
Національний авіаційний університет
м. Київ

ЗАХИСТ ІНФОРМАЦІЇ НА АВТОМАТИЗОВАНОМУ РОБОЧОМУ МІСЦІ

21 століття-це пік інформаційних технологій. Оскільки це включає в себе не тільки розробку і популяризацію техніки серед людей, її захист, то буде доцільним розглянути оцінку захищеності автоматизованого робочого місця,за яким працює кожен користувач. Зростаюча автоматизація процесів на зараз дозволяє сконцентрувати трудові зусилля на сфері інтелектуального виробництва, створення інформаційних продуктів і послуг, щоб полегшити життя людей і максимально швидко вирішувати проблеми.

Буде доцільним зауважити, що автоматизоване робоче місце (АРМ) - це програмно-технічний комплекс, що забезпечує автоматизацію функцій його діяльності, поєднуючи комплекс технічних, програмних, інформаційних та інших засобів. АРМ об'єднує програмно-апаратні засоби, що забезпечують взаємодію фахівця з ПК, надає можливість введення інформації та її виведення на екран монітору, принтер або інші пристрої[1]. Логіка цієї системи побудована таким чином, щоб максимально скоротити трудомісткість процесу і стерти межу між користувачем та апаратними пристроями. Через це, АРМ забезпечує робітника всіма засобами,щоб легко оперувати пристроями вводити інформацію за допомогою клавіатури, сканеру, та виводити її на екран монітора, принтера або звукову плату. Ці засоби установлені безпосередньо на робочому місці користувача, що використовується для автоматизації операцій взаємодії робітника з комп'ютером у процесі проектування та реалізації завдань.

З найдавніших часів будь-яка діяльність людей ґрунтувалася на отриманні та володінні інформацією, тобто на інформаційному забезпеченні. Саме інформація є одним з найважливіших засобів вирішення проблем і завдань, як на державному рівні, так і на рівні комерційних організацій і

окремих осіб. Але так як отримання інформації шляхом проведення власних досліджень і створення власних технологій є досить дорогим, то часто вигідніше витратити певну суму на добування вже існуючих відомостей. Таким чином, інформацію можна розглядати як товар. А бурхливий розвиток техніки, технології та інформатики в останні десятиліття викликало ще бурхливий розвиток технічних пристроїв і систем розвідки. У створення пристроїв і систем ведення розвідки завжди вкладалися і вкладаються величезні кошти в усіх розвинених країнах[2].

Все це пов'язано з достатнім ризиком цінності різного роду інформації, розголошення якої може призвести до серйозних втрат в різних областях (адміністративної, науково-технічної, комерційної і т.д.). Тому питання захисту інформації (ЗІ) набувають все більш важливе значення.

Метою несанкціонованого збору інформації в даний час є, перш за все - комерційний інтерес. Як правило, інформація різнохарактерна і різної цінності, ступінь її секретності (конфіденційності) залежить від особи або групи осіб, кому вона належить, а також сфери їх діяльності. Особливістю захисту мовної інформації є те, що вона не матеріальна, тому захищати її чисто технічними засобами складніше, ніж секретні документи, файли та інші носії інформації [3].

У цій доповіді розглядаються проблеми організації захисту кабінету керівника від НСД, а також аналізуються можливі дії зловмисника спрямовані на дестабілізацію цілісності, конфіденційності, доступності інформації. Крім цього, розглядаються основні методи протидії від дестабілізуючих факторів, а також дається оцінка ефективності їх застосування.

Література:

1.Інформаційні системи і технології на підприємствах - Плескач В.Л. - «Типи АРМ офісних систем» - Єл.Вид.

2.uk.wikipedia.org/wiki/Автоматизоване_робоче_місце

3.pidruchniki.com/1374121047746/informatika/avtomatizovane_roboche_mistse_fahivtsya_osnovni_funktsiyi_komponenti

Червінко Л.П.
Національний авіаційний університет
м. Київ

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

Модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;

·Підміна авторства інформації.

Для забезпечення секретності застосовується шифрування, або криптографія, що дозволяє трансформувати дані в зашифровану форму, з якої витягти вихідну інформацію можна тільки при наявності ключа.

В основі шифрування лежать два основних поняття: алгоритм і ключ. *Алгоритм* – це спосіб закодувати початковий текст, в результаті чого виходить зашифроване послання. Зашифроване послання може бути інтерпретовано тільки за допомогою *ключа.*

Оскільки таке важливе місце в системах шифрування приділяється секретності ключа, то основною проблемою подібних систем є генерація і передача ключа. Існують дві основні схеми шифрування: *симетричне шифрування* (його також іноді називають традиційними або шифруванням з секретним ключем) і *шифрування з відкритим ключем* (іноді цей тип шифрування називають асиметричним).

При *симетричному шифруванні* відправник та одержувач володіють одним і тим же ключем (секретним), за допомогою якого вони можуть зашифровувати і розшифровувати дані. При симетричному шифруванні використовуються ключі невеликої довжини, тому можна швидко шифрувати великі об'єми даних. Симетричне шифрування використовується, наприклад, деякими банками в мережах банкоматів. Недоліки симетричного шифрування: дуже складно знайти безпечний механізм, за допомогою якого відправник та одержувач зможуть таємно від інших вибрати ключ, тому і виникає проблема безпечного розповсюдження секретних ключів, а також для кожного адресата необхідно зберігати окремий секретний ключ. У схемі симетричного

шифрування неможливо гарантувати особу відправника, оскільки два користувача володіють одним ключем.

Недоліком асиметричного шифрування є необхідність використання більш довгих, ніж при симетричному шифруванні, ключів для забезпечення еквівалентного рівня безпеки, що позначається на обчислювальних ресурсах, необхідних для організації процесу шифрування.

Електронні підписи створюються шифруванням контрольної суми та додаткової інформації за допомогою особистого ключа відправника. Таким чином, будь-хто може розшифрувати підпис, використовуючи відкритий ключ, але корректно створити підпис може тільки власник особистого ключа. За допомогою електронного підпису одержувач може переконатися в тому, що отримане ним повідомлення надіслано не сторонньою особою, а мають певні права відправником. Для захисту від перехоплення та повторного використання підпис містить у собі унікальне число - порядковий номер.

Аутентифікація є одним з найважливіших компонентів організації захисту інформації в мережі. При аутентифікації використовується, як правило, принцип, що отримав назву "що він знає", - користувач знає деякий секретне слово, яке він посилає серверу аутентифікації у відповідь на його запит. Однією зі схем аутентифікації є використання стандартних паролів.

Для захисту корпоративних інформаційних мереж використовуються брандмауери. Брандмауери – це система або комбінація систем, що дозволяють розділити мережу на дві або більше частин і реалізувати набір правил, що визначають умови проходження пакетів з однієї частини в іншу. Як правило, ця межа проводиться між локальною мережею підприємства і INTERNET, хоча її можна провести і всередині. Брандмауер пропускає через себе весь трафік і для кожного пакету приймає рішення – пропускати його або відкинути.

Література:

1. Кузнєцов О.О. Захист інформації в комп'ютерних мережах - Х.: Айтек., 2013. - 319с.

2. Інформатика: Базовий курс / С.В. Симонович та ін - СПб.: Пітер, 2002. - 640с.: Іл.

3. Молдовян А.А., Молдовян Н.А., Рад Б.Я. Криптографія. - СПб.: Видавництво "Лань", 2001. - 224с., Іл. - (Підручники для вузів. Спеціальна література).

Довженко Н.М., Срочинская А.С.,
Государственный университет
Телекоммуникаций,
г. Киев

ЗАЩИТА ДАННЫХ В БЕСПРОВОДНЫХ СЕТЯХ WI-FI

Рассмотрены методы ограничения доступа, аутентификации и шифрования. Методы ограничения доступа представляют собой фильтрацию MAC-адресов и использование режима скрытого идентификатора SSID (Service Set IDentifier).

THE DATA PROTECTION IN WI-FI NETWORKS

N.Dovzhenko,
A.Srochinskaya

In this article were described methods of restricting access, authentication and encryption. Access control methods are providing by filtering of MAC-addresses and using modes of hidden the SSID identifier.

Фильтрацию можно осуществлять тремя способами:

- Точка доступа позволяет получить доступ станциям с любым MAC-адресом;
- Точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;
- Точка доступа запрещает доступ станциям, чьи MAC-адреса находятся в “чёрном списке”.

Режим скрытого идентификатора SSID основывается на том, что для своего обнаружения точка доступа периодически рассылает кадры-маячки (англ. beacon frames). Каждый такой кадр содержит служебную информацию для подключения и, в частности, присутствует SSID. В случае скрытого SSID это поле пустое, т.е. невозможно обнаружение беспроводной сети и нельзя к ней подключиться, не зная значение SSID . Но все станции в сети, подключенные к точке доступа, знают SSID и при подключении, когда рассылают Probe Request запросы, указывают идентификаторы сетей, имеющиеся в их профилях подключений. Прослушивая рабочий трафик, можно с легкостью получить значение SSID, необходимое для подключения к желаемой точке доступа.

В сетях Wi-Fi предусмотрены два варианта аутентификации:

Открытая аутентификация (англ. Open Authentication), когда рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе MAC-фильтрации, т.е. по сути это защита на основе ограничения доступа, что не безопасно.

Аутентификация с общим ключом (англ. Shared Key Authentication), при котором используется статический ключ шифрования алгоритма WEP (англ. Wired Equivalent Privacy). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети. Алгоритм шифрования WEP – это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа. Организация WECA (англ. Wi-Fi Alliance) совместно с IEEE анонсировали стандарт WPA (англ. Wi-Fi Protected Access). В WPA используется TKIP (англ. Tempora Key Integrity Protocol, протокол проверки целостности ключа), который использует усовершенствованный способ управления ключами и покадровое изменение ключа. WPA также использует два способа аутентификации:

- Аутентификация с помощью предустановленного ключа WPA-PSK (англ. Pre-Shared Key) (Enterprise Autentification);
- Аутентификация с помощью RADIUS-сервера (англ. Remote Access Dial-in User Service).

В сетях Wi-Fi используются следующие методы шифрования:

- WEP-шифрование (англ. Wired Equivalent Privacy) – аналог шифрования трафика в проводных сетях. Используется симметричный потоковый шифр RC4 (англ. Rivest Cipher 4), который достаточно быстро функционирует. На сегодняшний день WEP и RC4 не считаются криптостойкими.
- TKIP-шифрование (англ. Temporal Key Integrity Protocol) – используется тот же симметричный потоковый шифр RC4, но является более криптостойким. С учетом всех доработок и усовершенствований TKIP также не считается криптостойким.
- CKIP-шифрование (англ. Cisco Key Integrity Protocol) – имеет сходство с протоколом TKIP. Создан компанией Cisco. Используется протокол CMIC (англ. Cisco Message Integrity Check) для проверки целостности сообщений.
- WPA-шифрование – вместо уязвимого RC4, используется криптостойкий алгоритм шифрования AES (англ. Advanced Encryption Standard). Возможно использование EAP (англ. Extensible Authentication Protocol, расширяемый протокол аутентификации). Есть два режима: Pre-Shared Key (WPA-PSK) - каждый узел вводит пароль для доступа к сети и Enterprise - проверка осуществляется серверами RADIUS.

- WPA2-шифрование (IEEE 802.11i) – принят в в 2004 году, с 2006 года WPA2 должно поддерживать все выпускаемое Wi-Fi оборудование. В данном протоколе применяется RSN (англ. Robust Security Network, сеть с повышенной безопасностью). Изначально в WPA2 используется протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика). Основой является алгоритм AES. Для совместимости со старым оборудованием имеется поддержка TKIP и EAP (англ. Extensible Authentication Protocol) с некоторыми его дополнениями. Как и в WPA есть два режима работы: Pre-Shared Key и Enterprise.

Література

1. Петр Хенкин, Ольга Трофимова. Защита данных в сетях LTE

2. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей / Горячая линия - Телеком, 2008. – 288 с.

3. Fernandez, E.B. & VanHilst, M., Chapter 10, WiMAX Standards and Security (Edited by M. Ilyas & S. Ahson) / CRC Press Web site 2007

Заяц О.А.
Національний авіаційний університет
м. Київ

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ПРИ ВИРІШЕННІ ЗАДАЧ КІБЕРБЕЗПЕКИ

Зростання інформаційних зумовило не тільки швидкий розвиток і ефективне застосування інформаційних мереж в підприємницькій діяльності та в повсякденному житті, а й зростання нових загроз. Анонімність глобальних інформаційних мереж, швидкість передачі інформації і простота їх використання, - те, що є основними причинами технологічного буму і проникнення мережі Інтернет в усі сфери життя, - одночасно дозволяє використовувати всі ці переваги для вчинення протиправних діянь.

Кіберзлочинність – це злочинність у так званому кіберпросторі, який створений і (або) сформований таким чином: комп`ютери, комп`ютерні системи, мережі, їхні комп`ютерні програми, комп`ютерні дані, дані контенту, рух даних, і користувачі. В даний час офіційне визначення кіберпростору на міжнародному рівні відсутнє, втім, як і визначення кіберзлочинності. Кіберзлочини поділяють на види залежно від об`єкта, від предмета посягання, залежно від способів скоєння і т. п.

У першу группу виділено злочини протии конфіденційності, цілісності та доступності комп`ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

У другу группу входять злочини, пов`язані з використанням комп`ютера, як засобу скоєння злочинів - а саме, як засіб маніпуляцій з інформацією. У цю группу входять комп`ютерне шахрайство та комп`ютерне підроблення.

Третю группу складають злочини, пов`язані з контентом (змістом даних). У цю группу входять злочини, пов`язані з контентом - тобто з вмістом даних, розміщених в комп`ютерних мережах. Найпоширеніший і караних практично у всіх державах вигляд цих кіберзлочинів - злочини, пов`язані з дитячою порнографією.

У четверту группу увійшли злочини, пов`язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав.

П`ята группа злочинів зафіксована в окремому протоколі – це акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж.

У рамках інформаційного забезпечення національної безпеки, захисту особистої інформації є боротьба з кіберзлочинністю. Для найбільш повного захисту до цього процесу залучається все більше інтелектуальних технологій:

- інформаційні технології інтелектуального управління автономними мобільними кібернетичними системами;
- зорові інформаційні технології, призначені для сприйняття та розпізнавання зображень;
- мовленнєві інформаційні технології, призначені для сприйняття, розпізнавання та синтезу природної людської мови;
- знання, орієнтовані інформаційні технології, призначені для аналізу, розуміння, інтерпретації, генерації текстовоїі нформації, та цифрові технології змістовної обробки текстової інформації;
- інформаційні нейромережеві технології для ефективної обробки знань.

Література:

1. Башмаков А. И., Башмаков И. А. Интеллектуальные информационные технологии: Учеб.пособие. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2005. — 304 с

2. uk.wikipedia.org/wiki/Інформаційні_злочини

3. Роберт І. Сучаснііінформаційнітехнологіїосвіти [Текст] / І.Роберт. — М. : Школа-Пресс, 2004. — 454 с.

4.

Ю. Лапінський, А.Каплуненко
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ

У сучасних умовах успішне функціонування і розвиток підприємств все більше залежать від забезпечення інформаційної безпеки. Інформація відіграє вирішальну роль як у сфері виробництва, бізнесу та підприємництва, так і в ході конкурентної боротьби.

Особливе місце займають органи державного управління, де інформація нерідко носить таємний характер, і її захист повинен здійснюватись у суворій відповідності з державними нормативними актами у цій сфері. Одним з напрямків забезпечення інформаційної безпеки є захист інформації з обмеженим доступом, яка озвучується (під час проведення нарад, показів зі звуковим супроводом відеофільмів тощо) або здійснюється обробка технічними засобами акустичної інформації (системи звукопідсилення, засекречений зв'язок, у т.ч. урядовий зв'язок тощо).

Захист мовної інформації – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини).

Мовний сигнал – складний фізичний процес, пов'язаний зі зміною акустичних параметрів, які містять інформацію про зміст повідомлення .Мовний сигнал створюється голосовим апаратом людини і являє собою обурення повітряного середовища у вигляді хвиль стиснення і розтягнення (акустичні коливання). Енергія мовного сигналу зосереджена в діапазоні 300 - 4000 Гц.

Усвоєму первісному вигляді мовний сигнал в приміщенні присутній у вигляді акустичних і вібраційних коливань.

Залежно від середовища поширення сигналів і способів їх перехоплення технічні канали витоку мовної інформації можна розділити на:

Акустичні- за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали);

Вібраційні (віброакутсичні) - за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи вібрації (огороджувальні конструкції (стіни, стелі, підлоги, вікна, двері, короба вентиляційних систем тощо), інженерні комунікації (труби водопостачання, опалення, кондиціонування тощо));

Акустоелектричні - за рахунок впливу звукових коливань на ДТЗС (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля,створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»);

Оптико-електронні (лазерні канали) канали - за рахунок приймання та демодуляції відбитого відвібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання;

Параметричні - за рахунок впливу звукових коливань на ОТЗ і ДТЗС (за рахунок паразитної модуляції інформаційним сигналом випромінювань гетеродині в радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори, за рахунок утворення вторинних радіохвиль, при «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу);

При проведенні робіт із технічного захисту інформації одночасно, з використанням одних і тих же приладів, методик та спеціалістів можуть

здійснюватися заходи із захисту декількох каналів витоку інформації. Так, при проведенні робіт із захисту інформації від витоку акустичним каналом можуть проводитися роботи із захисту інформації від витоку віброакустичним і оптоелектронним каналами. Аналогічним чином здійснюються роботи із захисту інформації від витоку акустоелектричним та параметричним каналами побічних електромагнітних випромінювань та наводок (канали побічних електромагнітних випромінювань та наводок).

Виходячи з цього види роботи з технічного захисту інформації доцільно проводити за наступними напрямками:

- Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами;
- Захист інформації від витоку акустоелектричними та параметричними каналами;
- Захист інформації від витоку через закладні пристрої.

Для захисту мовної інформації з обмеженим доступом від витоку технічними каналами на об'єктах інформаційної діяльності створюється комплекс ТЗІ.

Використана література

1. *Інтернет ресурс www.tzi.ua*
2. *Інтернет ресурс www.tzi.com*
3. *Інтернет ресурс www.nauka.com.ua*

Мельниченко С. С.,
Государственный университет телекоммуникаций,
Учебно-научный институт защиты информации,
г. Киев

СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Системы контроля доступа – это программно-аппаратные комплексы, предназначенные для организации санкционированного прохода на охраняемые территории. Такие системы состоят их управляющих и исполнительных устройств, а также электронных ключей пользователей. Другим Иначе говоря, СКД – это автоматизированный комплекс специальных преград, которые открываются электронными ключами.

В случае разрешения доступа система приводит в действие исполнительные устройства, открывая проход для людей или въезд для автотранспорта. В противном случае доступ блокируется, включается сигнализация, и о попытке несанкционированного проникновения оповещается охрана.

К системе контроля доступа относятся такие устройства, как:

- контроллеры;

- приборы считывания (считыватели);
- идентификаторы физических носителей (карточки, ключ, радиобрелок), цифровых паролей, а также устройства распознавания биометрических параметров (отпечатков пальцев, сетчатки глаза);
- системы учета рабочего времени;
- ПО (программное обеспечение);
- исполнительные устройства.

Устройства для контроля доступа — виды

Контроллеры

Одними из центральных устройств, принадлежащих к системам контроля доступа и учета рабочего времени являются контроллеры. Эти приборы получают информацию со считывателей, осуществляя управление автоматикой блокировки дверей, замков, и т.д. Между собой контроллеры соединяются специальной информационной шиной. Ограничений по количеству зон систем контроля доступа, а также количеству исполнительных устройств практически не существует.

Считыватели

Считыватели – это устройства, предназначенные для идентификации личности человека и передачи информации о нем контроллеру, который принимает решение о доступе. На сегодняшний день существуют карточные, дактилоскопические и биометрические считыватели. Совместное использование системы контроля доступа и видеонаблюдения предоставляет возможность сравнивать информацию о владельце карточки с изображением на видео с камеры.

Идентификаторы

В системах контроля доступа используются контактные (таблетки «TouchMemory») и бесконтактные карточки (PROXIMITY). На таких карточках хранится информация о владельце, которая передается считывателю, обеспечивающему доступа на объект. В сложных системах контроля доступа владельцам карт предоставляют доступ не на все участки территории, которая охраняется. Каждый идентификатор предоставляет определенный уровень доступа, определяющий право прохода на тот или иной участок.

Система учета рабочего времени

Для учета времени нахождения сотрудника на рабочем месте, формирования отчетов для руководства компании предназначены специальные программно-аппаратные комплексы — системы учета рабочего времени. Такие системы позволяют автоматизировать процесс контроля сотрудников и обеспечить отделы фирмы достоверной информацией о времени нахождения работника в офисе (на предприятии).

Программное обеспечение

Программное обеспечение современных систем контроля доступа позволяет

настраивать все входящие в нее устройства: контроллеры, идентификаторы, считыватели и т.д., а также хранить данные о владельцах карт, производить отчеты о пребывании сотрудников на рабочем месте.
ПО для системы контроля доступа имеет повышенную надежность кода, сертифицировано согласно международным стандартам качества, а также обеспечено имеет всеми необходимыми гарантиями от программных сбоев и других неполадок оборудования.

Исполнительные устройства контроля доступа

- Электромагнитные замки – открытие таких устройств происходит посредством снятия напряжения. Недорогие и удобные замки.
- Электромеханические замки – отличаются высокой устойчивостью ко взлому, благодаря механической прочности и мощному ригелю.
- Электромеханические защелки – позволяют надежно удерживать двери в запертом состоянии. Легко устанавливаются на любые типы дверей
- Турникеты – монтируются на входе предприятия. На сегодняшний день выпускают различные виды турникетов: турникет-трипод, тумбовый турникет-трипод, роторный полуростовый турникет, роторный полноростовый турникет.
- Шлагбаумы – устанавливаются при въезде на территорию предприятия или автостоянку. Различаются по интенсивности использования и длине стрелы.

Типы систем контроля доступа

Системы контроля доступа подразделяются на два типа: автономные и сетевые.

- Автономные системы позволяют контролировать только одну точку доступа и не взаимодействуют с другими контроллерами. Контроллер и считыватель чаще всего совмещены в таких системах, к ним подключается электромагнитный или электромеханический замок, кнопка выхода, а также аккумулятор.
- В сетевых системах контроллеры не соединены между собой. Программирование, мониторинг, обмен информацией происходит через компьютер, на котором установлено специальное программное обеспечение. Данные системы позволяют приращивать число контроллеров, считывателей, пользователей и разделять функции между различными службами.

Література

1. *Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2009. - 496 с.*
2. *Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. - М.: Нолидж, 2009. - 496 с., ил.*
3. *Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия -Телеком, 2008. - 452 с.*

4. *Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред.А.П. Леонова. - Минск: АРИЛ, 2010. - 552*
5. *Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. - М.: Академический проект: Трикста, 2007. - 544 с.*

Мукосій В.С.
Національний авіаційний університет
м. Київ

ЗАХИСТ ДЕРЖАВНИХ РЕСУРСІВ ВІД КІБЕРНЕТИЧНОГО ВПЛИВУ

У наші часи дуже гостро стоїть питання захисту державних інформаційних ресурсів від кібернетичного впливу, особливо в останні роки, коли все більше увага звертається на захист інформації, що циркулює в кіберпросторі на території проведення антитерористичної операції. Саме поява концепцій ведення боротьби в кіберпросторі у складі збройних сил як України, так і сусідніх держав вказує на актуальність теми захисту державних інформаційних ресурсів, тому задля розкриття цієї теми було би доцільно, для початку, більш конкретно розтлумачити саме поняття таких ресурсів і можливого кібернетичного впливу на них.

Державні інформаційні ресурси поділяються на такі категорії:

- базові - інформаційні ресурси загального користування, включають загальнонаціональні реєстри і використовуються з метою інформаційного забезпечення державних органів, задоволення інформаційних потреб громадян і юридичних осіб;
- відомчі - містять інформацію, необхідну для інформаційного забезпечення державних органів відповідно до їх компетенції (а також для задоволення інформаційних потреб громадян і юридичних осіб);
- територіальні - містять інформацію, необхідну для інформаційного забезпечення місцевих виконавчих і розпорядчих органів відповідно до їх компетенції (а також для задоволення інформаційних потреб громадян і юридичних осіб).

Під кібернетичним впливом на такі ресурси розуміють сукупність взаємопов’язаних за метою і завданнями кібератак, спрямованих на реалізацію несанкціонованих дій з метою порушення порядку функціонування, змін властивостей інформації, отримання контролю над системою, копіювання, модифікації, вилучення, пошкодження, впровадження або знищення даних, створення умов для зміни поведінки користувачів, як в реальному так і в розподіленому масштабі часу, в тому числі з використанням закладних засобів.

Важливо відмітити, що на даний момент в Україні існує велика кількість факторів, що запобігають досконалому забезпеченню захисту державних інформаційних ресурсів від кібернетичного впливу. Серед цих факторів - дефіцитна, термінологічна, нормативно-правова невизначеність у сфері

кібернетичної безпеки, а також залежність держави від програмних та технічних продуктів іноземного виробництва. Однак важливість покращення захисту державного інформаційного кіберпростору має переважати подібні недоліки, тому розвиток має бути спрямований у такому напрямку, як:

- покращення антивірусного захисту;
- розробка комплексної системи захисту інформації;
- вдосконалення системи управління інформаційною безпекою;
- постійна перевірка відповідності систем захисту;
- навчання користувачів і підготовка фахівців.

Література:

1. Інформаційні ресурси з науки і технологій. Сухорукова. Р. М. http://ua-referat.com/Інформаційні_ресурси

2. Розширення термінології сучасного кіберпростору. Куцаєв В.В., Живило Є.О., Срібний С.П. Черниш Ю.О. http://mino.esrae.ru/pdf/2014/3Sm/1387.doc

3. Бондарчук А. П. Дослідження принципів системного підходу до проектування системи радіозв'язку //Наукові записки Українського науково-дослідного інституту зв'язку. – 2013. – №. 2. – С. 44-47.

4. *Сучасні підходи до забезпечення кібернетичної безпеки. М.В. Гайворонський* http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2015/05/Graivoronskyi-Present-Conf-IPT-2015.pdf

Платоненко А. В., аспірант
Державний університет телекомунікацій,
м. Київ

АКТУАЛЬНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ МОБІЛЬНИХ ПРИСТРОЇВ У МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

Розглянуто вразливості сучасних мобільних пристроїв з використанням мереж нового покоління, адже кожен третій житель України має смартфон з сенсорним екраном, а висока швидкість передачі даних є зручною не тільки для користувача, а і для зловмисника, що несе за собою небезпеку для інформації, яка зберігається та передається з використанням мобільних пристроїв.

Сучасні мобільні пристрої стали невід’ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається [1]. Швидкість передачі даних у мережах 4G, яка може досягати до 1 Гбіт/с (в 6 разів більше у порівнянні з найшвидшими мережами 3G), а в мережах 5G

швидкість передачі даних може досягати до 5 Гбіт/с (в 80 разів більше ніж заявлена максимально можлива швидкість в мережах 3G-операторів України). З використанням високошвидкісних мобільних мереж нового покоління, загрози інформаційної безпеки для державних та приватних установ [2] збільшуються, адже для зловмисників відкриваються більші технічні можливості, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи, а не тільки для спілкування.

Кожен третій житель України (33%) має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – половина (50%). Порівняно з 2015 роком простежується зростання частки таких людей – з 26% до 33% у випадку загального населення і з 41% до 50% у випадку осіб до 50 років. Якщо серед молоді 65% користуються смартфонами, то серед осіб літнього віку – 5%. Типовий користувач смартфонів – це молода особа не старше 40 років з вищою освітою, яка проживає у середніх і великих містах України. Більшість (66%) користуються операційною системою Android, а 68% користувачів смартфонів мають досвід встановлення додатків. Найбільш популярними є соціальні мережі – 73%, ігри – 61%, навігація – 51%, месенджери – 49% [3]. Нажаль неуважні або недосвідчені користувачі мобільних пристроїв встановлюють і зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисник може отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, його можливості збільшуються в рази. Рівень розкриття кіберзлочинів в Україні становить в середньому 50%, при цьому 80% постраждалим вдається відшкодувати збитки, яких вони зазнали внаслідок дій злочинців. Структура кіберзлочинів в Україні має такий вигляд:

- 65% - шахрайство в інтернеті (обман покупців під час онлайн-шопінгу та ін.);
- 16% - хакерські атаки (викрадення інформації, блокування роботи систем);
- 13% - злочини з платіжними системами (скімери, дублікати карток, зараження вірусами);
- 5% - нелегальний контент (поширення матеріалів з порушенням авторських прав).

В свою чергу, кількість сім-карт на ринку продовжує зменшуватись, незважаючи на продаж великої кількості смартфонів на дві сім-картки (більше 90%) можна зробити висновок, що користувачі стали більше приділяти увагу економії у використанні ресурсів мережі та більш сумлінно відноситись до можливостей своїх пристроїв. Таким чином, це можна вважати певним обмеженням для зловмисників, хоча і не суттєвим. Для більш ефективного захисту треба бути уважнішим, використовувати перевірене програмне

забезпечення, різні паролі для облікових записів, блокування пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати. Це допоможе ефективно та безпечно використовувати можливості мереж нового покоління.

Література:

1. *Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах/ А. В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р.*

2. *Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко, Київ, ДУТ, Сучасний захист інформації. Науковий журнал. – 2015. – № 4, с. 86 – 90.*

3. *Використання смартфонів в Україні [Електронний ресурс] – Режим доступу: http://lead9.com/slide/slide.pdf*

***Рабчун Д.И.**, аспирант*
Государственный университет телекоммуникаций
г. Киев

АНАЛИЗ ПРОБЛЕМЫ УПРАВЛЕНИЯ РЕСУРСАМИ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В МОБИЛЬНЫХ СЕТЯХ НОВОГО ПОКОЛЕНИЯ В УСЛОВИЯХ ДИНАМИЧЕСКОГО ИНФОРМАЦИОННОГО ПРОТИВОСТОЯНИЯ

В докладе рассмотрены основные проблемы, связанные с управлением ресурсами программных средств защиты информации.

Стоит отметить, что мобильные сети — это сложная информационная инфраструктура, в которую входят так же классические компьютерные сети и серверное оборудование.

Сегодня одним из самых популярных подходов к защите именно таких информационно телекоммуникационных сетей (ИТС) является использование программных средств защиты информации.

Исторически первыми решениями, которые стали на страже сетевой безопасности были межсетевые экраны. Впоследствии, вместе с ростом требований бизнеса к защите информации, к ним добавились технологии виртуальных частных сетей. В то же время, вместе с популярностью информационных сетевых технологий активизировался рост хакерских атак, что побудило разработку IDS/IPS-систем. Параллельно с этими решениями на защиту периметра сети вставали средства для борьбы со спамом и вирусами, а также WEB-фильтры. С течением времени средства защиты ИТС пополнились за счет систем контентной фильтрации, DLP-систем и WAN-оптимизаторов. Однако затем стали проявляться проблемы их совместного использования, управления и владения подобными накоплениями программных средств. Поиск решения этих проблем привел к появлению UTM-систем.

Анализируя доступные материалы, предоставленные аналитическими агентствами и вендорами UTM-систем можно выделить два основных подхода к построению современных комплексов ПСЗИ для ИТС: фрагментарный и комплексный.

Основной принцип первого подхода базируется на том, что специализированное программное средство защиты более эффективно, чем универсальное. Но, вместе с увеличением функционала таких средств начали проявляться и недостатки совместного использования различных ПСЗИ. Так, за счет независимости каждого компонента комплексов ПСЗИ происходит дублирование функций защиты, что приводит к существенному уменьшению оперативности функционирования системы в целом, росте сложности администрирования (управления) и росте совокупной стоимости такого рода защиты. Кроме того, обычно неизвестно каким образом продукты различных производителей будут взаимодействовать друг с другом, что создает дополнительные трудности при установке, управлении и обслуживании этих систем. Система защиты на основе такого подхода не позволяет консолидировать информацию от различных ПСЗИ, что делает невозможным ее анализ. В то же время, с точки зрения бизнеса – решение для программного обеспечения информационной безопасности должно быть эффективным не только по показателям защищенности информации, но и с точки зрения стоимости, что позволит уменьшить затраты на защиту с одной стороны, но не привести к усложнению системы с другой.

Как решение поставленных проблем были предложены системы защиты ИТС нового класса: UTM, NGFW, NGIPS и другие. Все перечисленные системы можно охарактеризовать одной, отличительной от традиционных средств защиты чертой: все они включают элементы системы управления программными средствами защиты информации. Под этим понимается, что комплексность в вышеупомянутых системах достигается за счет набора программных средств защиты информации: Firewall, Application control, IPS, DLP, WAF, Anti- virus, которые выполнены на единой платформе и консолидированы единым набором управляющих команд [1].

Рассмотрим, что вкладывается в определение UTM-системы в настоящее время. Аналитическое агентство IDC под универсальным шлюзом безопасности (Unified Threat Management, UTM), подразумевает такое устройство, которое имеет следующий минимальный набор функций:

- Брандмауэр;
- Система обнаружения и защиты от вторжений (IDS / IPS)
- Virtual Private Network (VPN)
- Антивирус.

По мнению агентства Gartner UTM-система должна обеспечивать:

- Стандартные функции межсетевого экранирования с контролем состояний сетевых соединений;
- Возможность организации удаленного доступа по VPN;

- Функциональность WEB-шлюза безопасности с проверками на наличие вредоносного трафика, URL-фильтрацией и контролем приложений;

- Предотвращение сетевых вторжений.

Объединение традиционных ПСЗИ в интегрированные UTM-системы дает возможность операторам мобильной связи перейти на новый более высокий уровень защиты информации в своих ИТС. Использование полноценных комплексов ПСЗИ определяет особую актуальность в настоящее время, когда ежедневно появляются новые, все более разнообразные и изысканные виды угроз.

В то же время практически во всех проанализированных комплексах ПСЗИ выявлено отсутствие своевременной адекватной реакции на изменение условий информационного противостояния, то есть гибкость в настройке уровня защиты системы не используется в должном объеме, возлагая все настройки на администратора безопасности, что значительно влияет на эффективность их применения [2].

Таким образом в приведенном анализе современных подходов к защите информационно телекоммуникационных сетей программными средствами защиты информации можно выделить следующие проблемные места и недостатки:

1. UTM система является единой точкой отказа на входе ИТС. Тем не менее вероятность отказа такого устройства невелика;

2. Возможное влияние функционирования UTM системы на скорость работы ИТС если UTM устройство не поддерживает максимально возможную в сети скорость;

3. Отсутствие своевременной адекватной реакции на изменение условий информационного противостояния, то есть гибкость в настройке уровня защиты системы не используется в должном объеме, возлагая все настройки на администратора безопасности.

Литература

1. *Worldwide Quarterly Security Appliance Tracker // IDC Tracker. – 2015.*
2. *Рабчун Д.І. Логіко-динамічна модель процесу управління ресурсами захисту в умовах інформаційного протистояння / Д.І. Рабчун // Сучасний захист інформації: наук.-практ. журнал, 2016. — №3. — С. 62-67*

Трапезнікова В.П.
Національний авіаційний університет
м. Київ

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Ми живемо у час швидкого розвитку інформаційних мереж та систем, широкого застосування комп’ютерних ехнологій в автоматизованих системах обробки інформації. На перший погляд зникає проблема усної передачі інформації, коли її дуже легко перехопити, протее виникає така сама проблема, але вже в інформаційному просторі.

На даний момент дуже гостро стоїть питання проблеми захисту інформації, що циркулює в інформаційних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаною з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку

Фізична безпека інформаційних ресурсів направлена, в першу чергу, на попередження неавторизованого доступу, пошкодження та вплив у відношенні до приміщень та інформації, а також на забезпечення безпеки засобів обробки критичної службової інформації, за допомогою використання різноманітних засобів контролю проникнення, а також захисних бар’єрів.

Для того, щоб побудувати фізичну безпеку інформаційної системи, треба розуміти основні загрози безпеці, а також методи їх вирішення.

Фізичний захист інформації на сьогодні включає наступні основніз асоби:

пасивні – до них відносяться інженернічи фізичні засоби, що контролюють прилади ліній зв’язку;

активні – до них відносяться скремблери, шумогенератори, засоби для маскування даних.

На даний час найнадійнішими системами безпеки вважаються системи, що мають структурність. Тому на практиці, для захисту інформації від витоку, треба застосовувати одразу декілька пристроїв, що відповідають за безпеку. На разі, вибір таких пристроїв дуже великий та різноманітний, тому в данному випадку є декілька можливих шляхів:

підібрати найбільш оптимальний пристрій, що можна використовувати автономно;

підібрати декілька пристроїв, що будуть використовуватися комплексно за допомогою блоку керування універсального характеру;

використовувати готовий набір пристроїв.

Отож, хоча зараз стрімко розвиваються інші види захисту інформації, такі як криптографічний, програмний, проте не варто недооцінювати важливість фізичної безпеки інформації - вона є першим кроком до повноцінного захисту інформації.

Література:

1. Домарев В.В. Безопасность информационных технологий. Системный подход. – Изд-во: ТИД «ДС». – 2007. – 292с.

2. Хорошко В.А. Модель системы защиты иформации. ”Захист інформації”.-№1, 1999.

3.

Возная О.Т.
Государственный университет телекоммуникаций
г. Киев

5G В ЭВОЛЮЦИИ АВТОМОБИЛЕЙ

Самоуправляемые транспортные средства – еще одна область, реализация которой потребует сетей связи нового поколения. Автомобили можно будет оснастить сенсорами, считывающими всевозможную информацию о дорожной обстановке: ближайших транспортных средствах, погодных условиях, состоянии асфальта, дорожных знаках и др. На основе этих данных управление поездкой можно осуществлять в автоматическом режиме.

Помимо удобства для водителя машины, оснащение сенсорами автомобилей открывает новые возможности для повышения безопасности на дорогах. По сетям 5G автомобили смогут коммуницировать между собой и принимать мгновенные решения, что делать в той или иной ситуации на основе информации, полученной от других транспортных средств на дороге. Например, автомобиль мог бы пересылать сигнал о своем резком торможении, так чтобы машина, с которой из-за этого угрожает столкновение, могла также резко затормозить в автоматическом режиме. В сетях 4G реализовать такой сервис небезопасно, поскольку задержка сигнала слишком велика, чтобы управлять автомобилем в режиме реального времени. В июне 2016 года ABI Research опубликовала прогноз, согласно которому к 2025 году около 67 млн автомобилей будут использовать сервисы 5G.

Три миллиона из них - самоуправляемые автомобили. Технология 5G, благодаря более быстрому отклику, станет предпочтительной для широкополосного потокового мультимедиа, отправки диагностической информации сервисному центру, использования в системах V2X (Vehicle-to-Everything — система обмена данными между автомобилем и другими объектами дорожной инфраструктуры, например, с автомобилями, дорожными знаками, разметкой, светофорами; инфраструктура также должна быть подключена к интернету).

Поддержка систем V2X – это одно из ключевых требований для подключённого транспортного средства будущего. Технология V2X тесно связана с понятием совместной мобильности, которая позволяет автомобилям обмениваться друг с другом различной информацией. 5G, благодаря более низкой задержке при установке соединения, сделает взаимодействие через V2X

более эффективным, а движение самоуправляемых автомобилей на интеллектуальных дорогах – более безопасным.

Чтобы технология V2X стала реальностью, две области – автомобильная и телекоммуникационная, должны расширить зону охвата 5G-сигнала и обеспечить уверенный приём. Ожидается, что это станет вполне реальным к 2025 году. 5G позволит мобильным операторам внедрить больше услуг с добавленной стоимостью для автомобильной экосистемы. Ожидают появления новых бизнес-моделей и новых возможностей для автомобильной отрасли благодаря низкой задержке при установке соединения – до 1 мс.

Литература:

1. Журнал CNews, 71 выпуск, "5G Как изменится мобильная связь в ближайшие 5 лет"? с. 51-55.

2. http://iot.ru/transportnaya-telematika/5g-prineset-novye-biznes-modeli-i-vozmozhnosti-dlya-avtomobilnoy-otrasli

Стрилецкий Д.Ф., студент
Государственный университет телекоммуникаций,
м. Киев

ВЛИЯНИЕ НОВЫХ ПОКОЛЕНИЙ МОБИЛЬНОЙ СВЯЗИ НА РЕШЕНИЕ ПРОБЛЕМ ОБЩЕСТВЕННОСТИ И ЛИЧНЫЙ ПРОЕКТ КАК ПРИМЕР

Возможности 4G и его скорость. Мессенджер Telegram и его инструмент для решения задач в виде ботов. DuttyBot – пример бота в реальной жизни на основе доступа к расписанию университета. Инструменты для разработки.

4G, как и его предшественники, как и его будущие последователи – это неизменный доступ к инструментам обмена информацией: передавать потоковое видео очень высокого качества, загружать большие файлы в мгновение ока и даже, в определенных условиях, использовать некоторые из этих сетей как замену DSL. К четвёртому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с — мобильным и 1 Гбит/с — стационарным абонентам.

Telegram – бесплатный кроссплатформенный мессенджер для смартфонов и других устройств, позволяющий обмениваться текстовыми сообщениями и медиафайлами различных форматов. Используется проприетарная серверная часть с закрытым кодом, работающая на мощностях нескольких компаний США и Германии, финансируемых Павлом Дуровым.

При помощи специального API сторонние разработчики могут создавать «ботов», специальные аккаунты, управляемые программами. Типичные боты отвечают на специальные команды в персональных и групповых чатах, также они могут осуществлять поиск в интернете или выполнять иные задачи, применяются в развлекательных целях или в бизнесе. В сентябре 2015 года Павел Дуров заявил о скором появлении возможностей монетизации и размещения рекламы в ботах.

DuttyBot – один из примеров ботов, созданный для решения проблемы недоступности расписания университета на мобильных устройствах. Пользователи могут иметь в распоряжении ряд функций: расписание на сегодняшний и завтрашний день, время пар, удобный интерфейс, отзывчивость автора, возможность оставить отзыв и предложения, а также следить за разработкой и новостями.

Для создания DuttyBot использовался язык программирования Python (версия 3.5+), разного рода API и библиотеки в свободном доступе, облачная платформа Heroku, базы данных PostgreSQL и разного рода дополнительный минорные инструменты.

Панкратова О.С., *аспирант*
Государственный университет телекоммуникаций,
г. Киев

АНАЛИЗ УСЛОВИЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН ДЛЯ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЙ 4G И 5G

Для высоких орбит космических аппаратов (КА) выше 200 км, территория Украины представляет один рассредоточенный пункт управления. Увеличение радиотехнических комплексов (РТК) повышает резервирование технических средств, но не изменяет технологию управления КА. В виду отсутствия национальных технических пунктов вне пределов Украины представляется целесообразным создание только однопунктных технологий управления КА. Особо это важно для КА выполняющих как народнохозяйственные, так и оборонные задачи. В связи с применением однопунктной технологии управления КА экономически целесообразно использовать один РТК или одно РТС поэтому появляется необходимость повышения помехоустойчивости РТК (РТС), в частности для обнаружения радиосигналов. Учитывая, что современные мировые тенденции направлены на практическое освоение см и мм диапазона длин волн. Возрастает роль практического использования этих диапазонов длин волн национальными техническими средствами. Поскольку тропосферный участок неотъемлемая часть прохождения большинства реальных сверхвысокочастотных (СВЧ) и крайне высокочастотных (КВЧ) радиосигналов КА, а особенности тропосферного распространения широкополосных сигналов см и мм

диапазонов изучены недостаточно полно, целесообразно провести анализ спецификации эффектов указанного выше распространения радиоволн и оценить их влияние на качество передачи информации. Рассмотрим особенности нижней части атмосферы - тропосферу - это наличие в ней гидрометеоров в жидком и твердом состояниях - капелек воды и снежинок. Для решения поставленной задачи систематизируем основные радиофизические явления происходящие при прохождении широкополосных СВЧ и КВЧ радиосигналов через тропосферу с указанием характера их влияния на эффективность функционирования сверхскоростных систем связи.

Результаты данной классификации представлены в таблице №1

№ п/п	**Наименование физического эффекта**	**Причины возникновения физического эффекта**	**Характер влияния на качество КВЧй связи**
1	*2*	*3*	*4*
1.1	Затухание сигналов	а) молекулярное затухание в “спокойной” тропосфере б) затухание в гидрометрах	Снижение энергетического потенциала То же
1.2	Рассеяние сигналов	а) рассеяние в гидрометрах б) турбулентное рассеяние	То же
1.3	Рефракция радиоволн	а) регулярная рефракция б) флуктуация коэффициента преломления	То же
1.4	Мерцания (сцилцилляции амплитуды и фазы) сигналов	а) мерцание вследствие рефракции радиоволн б) мерцание в турбулентностях в) мерцание в водных или льдосодержащих облаках	
1.5	Доплеровские искажения (смещение и деформации спектра) сигналов	Вариации коэффициента преломления волн в среде распространения	То же
1.6	Снижение пространственной и поляризационной избирательности антенн	Возрастание ошибок и потерь наведения антенн	То же
1.7	Уменьшение эффективного коэффициента усиления антенн	а) флюктуации угла прихода волны б) нарушение когерентности (фазовой декорреляции) сигналов по апертуре из-за фазовой дисперсии траекторий лучей	То же

1.8	Излучение (шум) тропосферы	а) излучение “спокойной” тропосферы б) излучение гидрометеоров в) излучение турбулентностей	Появление дополнительной помехи и искажений
1.9	Дифракция радиоволн	дифракция на рельефе местности	То же
1.10	Образование тропосферных волноводных каналов	а) приемные “волноводы” б) приподнятые “волноводы”	
1.11	Деполяризация радиоволн	а) деполяризация в гидрометеорах б) деполяризация в турбулентных образованиях в) деполяризация вследствие фарадеевских вращений г) деполяризация в водных или льдосодержащих облаках д) деполяризация вследствие многолучевого распространения	
1.12	Возрастание уровня внутри-межканальных помех	а) снижение пространственной и поляризационной избирательности антенн б) образование пространственных волноводных каналов в) дифракция на рельефе местности	
1.13	Многолучевое распространение	а) дискретная многолучевость (счетное множество)	Ограничение максимальной скорости лучей
1.14	Дисперсионные свойства тропосферы	а) амплитудная дисперсия вследствие неравномерного затухания в полосе частот сигнала б) амплитудно- фазовая дисперсия в турбулентных образованиях	То же
1.15	Возрастание уровня искажений сигналов	Увеличение потерь при оптимальной обработке сигналов вследствие ограничения полосы и радиуса когерентного тропосферного канала	

Перепелиця Ліна
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ОБ'ЄКТІВ МУЛЬТИМЕДІА

Питання збереження конфіденційності інформаційних потоків під час їх зберігання та передачі каналами зв'язку, стоїть на провідній позиції у процесі забезпечення інформаційної безпеки особистості, суспільства та держави. На сьогодні найбільш поширеними технологіями захисту інформації є процедури поєднанням криптографічних та стеганографічних методів (комбіновані).
Відповідно до обраного типу контейнера визначається метод приховування інформаційних потоків.

Приховування даних у просторовій області.

Загальний принцип таких алгоритмів полягає у заміні надлишкової, малозначної частини зображення бітами секретного повідомлення. Для витягу повідомлення необхідно знати алгоритм, по якому воно розміщувалося у зображенні.

1) Метод заміни найменш значущого біту.

Метод заміни найменш значущого біту - найбільш розповсюджений метод серед методів даного класу. НЗБ несуть у собі найменше інформації. Як відомо, людина, у більшості випадків, не може розрізнити інформацію у даних бітах. При чому в чорно-білому зображенні (в якому кожен піксель кодується одним байтом) об'єм вбудованих даних може займати до 1/8 об'єму зображення-контейнера. Популярність даного методу обумовлена його простотою та можливістю приховувати доволі великі об'єми даних. В більшості випадків цей метод працює із растровими зображеннями, представленими у форматі без компресії даних (GIF, BMP).

2) Метод псевдовипадкового інтервалу.

Даний підхід полягає у псевдовипадковому розподілення бітів повідомлення по зображенню-контейнеру, внаслідок чого відстань між двома вбудованими бітами визначається псевдовипадково. Цей підхід ефективний у випадку, коли об'єм повідомлення набагато менший за контейнер. Недоліком такого методу є те, що біти повідомлення розподіляються по контейнеру у тому ж порядку, що і у самому повідомленні.

3) Метод псевдовипадкової перестановки.

Основою цього методу є генератор псевдовипадкових чисел (ПВЧ), який формує певну псевдовипадкову послідовність індексів $j_1, j_2 \ldots j_k$ і *k-й* біт повідомлення зберігається у пікселі із індексом j_k .

Функція перестановки має бути псевдовипадковою і мати достатньо великий набір індексів, щоб жоден індекс не повторився жодного разу і не відбулося «перетину».Цей метод забезпечує рівномірний розподіл інформаційних бітів по контейнеру. Імовірність перетину зменшується із зменшенням співвідношення (довжина повідомлення)/(довжина контейнера).

4) Метод блочного приховування.

При використанні даного методу зображення-контейнер розбивають на блоки, що не перетинаються між собою. Для кожного блоку визначають певний біт парності. В кожному блоці приховують один секретний біт. Якщо визначений біт парності не відповідає секретному біту, проводять інвертування НЗБ блоку, доки біт парності не буде, по суті, секретним бітом.

Цей метод, як і всі попередні, має низьку стійкість до викривлень, але він має свої переваги – існує можливість модифікувати такий піксель у блоку, щоб статистика контейнера була змінена якомога менше.

5) Метод заміни палітри.

Ще один метод приховування даних у зображенні – зміна палітри кольорів. Палітра кольорів зображення зберігається у вигляді списку пар індексів (i, A_i) який визначає відповідність між індексом i та його вектором кольору. Кожному пікселю зображення ставиться у відповідність певний індекс у таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення зображення, конфіденційна інформація може бути прихована шляхом перестановки кольорів у палітрі.

Приховування даних у частотній області зображення.

Найпоширеніші методи приховування даних у частотній області використовують вейвлет-перетворення та дискретно-косинусне перетворення (ДКП). Це пояснюється широким їх розповсюдженням у технологіях компресії цифрових зображень.

1) Метод відносної заміни величин коефіцієнтів ДКП.

При використанні даного методу зображення розбивається на блоки 8х8 пікселів. До кожного з блоків застосовується ДКП, в результаті чого отримується матриця коефіцієнтів ДКП 8х8. Кожен блок призначений для приховування одного біту даних. Приховування проводиться заміною одного коефіцієнту у блоку.

2) Метод Бенгама-Мемона-Ео-Юнга.

Даний метод є модифікацією попереднього. Основною зміною є той факт, що при використанні даного методу секретна інформація приховується не в усіх блоках зображення, а тільки в обраних блоках (найбільш підходящих).

3) Метод Фрідріх.

Згідно цього методу, який по суті є комбінацією двох алгоритмів, секретні дані вбудовуються в низькочастотні та середньочастотні коефіцієнти ДКП. Каскадне використання цих двох алгоритмів може дати непогані результати відносно стійкості стеганографічної системи до різних атак.

4) Методи розширення спектру.

Система зв’язку є системою із розширеним спектром, коли:

· Полоса частот, яка використовується при передачі, значно ширша за необхідну для передачі повідомлення, за рахунок чого співвідношення сигнал/шум є доволі низьким, і повідомлення важко знайти у каналі (особливо розрізнити органам чуття людини);

· Розширення спектру відбувається за допомогою, так званого, розширюючого сигналу, який не залежить від інформації, що передається. Присутність енергії сигналу в усіх частотних діапазонах робить радіосигнал стійким до завад, а інформацію, що знаходиться у контейнері - стійкою до її видалення.

· Відновлення первинної інформації відбувається шляхом зіставлення отриманого сигналу та синхронізованої копії кодового(розширюючого) сигналу [1].

Приховування даних у аудіосигналах

Особливий розвиток отримали стеганографічні методи приховування інформації у аудіосередовищі.

1) Кодування найменш значущих бітів (часова область).

Даний метод є найпростішим серед методів приховування даних у аудіосигналах. Його суть полягає у заміні НЗБ у кожній точці вибірки із сигналу, представленого у двійковій послідовності. Використання даного методу обумовлює високу пропускну здатність каналу, платою за що є добре чутний низькочастотний шум. Дану проблему можна вирішити використанням записів, на яких і так присутній певний шум, наприклад, звук стадіону на живому концерті. Але, як і у аналогічних методах приховування інформації у нерухомих зображеннях, заповнені контейнери є вразливими до сторонніх впливів окрім випадків, коли секретна інформація вбудована із внесенням надлишковості. Однак, останнє при збільшенні стійкості каналу зменшує швидкість передачі даних.

2) Метод фазового кодування (частотна область).

Основною ідеєю методу фазового кодування є заміна фази вихідного звукового сегменту на деяку опорну фазу, характер зміни якої і відражає повідомлення, яке необхідно приховати. При правильному використанні даний метод є найефективнішим для приховування даних у аудіосигналах, оскільки, доки модифікація фази достатньо мала, наявність повідомлення може бути абсолютно не відчутно на слух (не враховуючи використання спецтехніки).

3) Метод розширення спектра (часова область).

Даний метод майже ідентичний до методу приховування даних у нерухомих зображеннях шляхом розширення спектру. Тобто, секретне повідомлення розподіляється по частотам несучого сигналу рівномірно, так щоб співвідношення сигнал(повідомлення)/шум у каналі було дуже низьким і не виникло підозр щодо наявності повідомлення. Сигнал-контейнер, в даному випадку, обирається набагато більший за секретне повідомлення.

4) Приховування даних із використанням ехо-сигналу.

Даний метод вбудовує повідомлення у аудіосигнал-контейнер шляхом введення у нього ехо-сигналу. Дані приховуються зміною параметрів ехо-сигналу: початкової амплітуди, швидкості затухання та зсуву. Коли зсув між оригінальним сигналом та ехо-сигналом зменшується, починаючи з певного значення, ССЛ стає нездатною виявити різницю між двома сигналами, а ехо-сигнал сприймається лише як додатковий резонанс. Цей метод непростий у реалізації, тому що це значення зсуву дуже важко визначити. Воно значною мірою залежить від якості початкового сигналу і, само собою, від слухача.

Приховування даних у відео даних

Стеганографічні методи приховування рідше всього використовуються у відеоданих, так як даний файл складається з динамічних зображень (фреймів) та звукової доріжки. Для цих цілей найчастіше використовуються контейнери у форматах MPEG – 2, MPEG – 4 та AVI. Варто також зазначити, що досі не використовується в якості контейнерів одночасно аудіо доріжки та фрейми.

На сьогодні існує три методи для приховування інформації у відеоданих , а саме:

Метод вбудовування на рівні коефіцієнтів – біти приховуваного повідомлення вбудовуються в коефіцієнти ДКП. Для зменшення внесених змін використовують додатковий спеціальний сигнал. В зв'язку з обмеженням бітової швидкості, при вбудовування змінюється лише 10-12% коефіцієнтів ДКП. При використанні даного методу приховувана інформація зберігається при фільтруванні, зашумленні (адитивним шумом) і дискретизації.

1) *Метод вбудовування інформації на рівні бітової площини* - цей метод відрізняється високою пропускною здатністю і легкими обчисленнями. Але є й істотний недолік: інформація, вбудована таким чином, може бути легко видалена. При повторному накладенні послідовності біт якість відео погіршиться незначним чином, а приховувана інформація буде знищена.

2) *Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами* - в снові цього методу лежить диференціальне вбудовування енергії. Цей метод може використовуватись для багатьох алгоритмів стиснення, не тільки для MPEG. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП.

Висновки

Стеганографічні системи захисту інформаційних потоків, під час їх зберігання та передачі займають провідній позиції у процесах забезпечення інформаційної безпеки. У роботі проведено аналіз існуючих стеганографічних методів.

Літаратура

1. Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009.
2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография //теория и практика/Г.Ф. Конахович, А.Ю. Пузыренко.—Киев: МК-Пресс. – 2006.
3. Моденова О. В. Стеганография и стегоанализ в видеофайлах //Прикладная дискретная математика. Приложение. – 2010. – №. 3.

Косенко Владислав
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ДЖЕРЕЛА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Джерела загроз інформаційній безпеці розуміються як вихідні підстави (причини) небезпечного впливу на життєво важливі інтереси особистості, суспільства і держави в інформаційній сфері.

За типом *джерела* загрози підрозділяються на такі, що мають *соціальний* і *природний* характер. Загрози соціального характеру проявляються в процесі взаємодії між соціальними спільнотами (групами), а природні загрози - взаємодії соціальних груп з навколишнім природним середовищем.

Залежно від *характеру прояву* небезпечного впливу на об'єкти інформаційної безпеки джерела загроз можуть носити зовнішній або внутрішній характер.

До *зовнішніх джерел* загроз інформаційної безпеки відносяться:

• діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур, спрямована проти інтересів Російської Федерації в інформаційній сфері;

• прагнення ряду країн до домінування і ущемлення інтересів Росії у світовому інформаційному просторі, витіснення її з зовнішнього і внутрішнього інформаційних ринків;

• загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами;

• діяльність міжнародних терористичних організацій;

• збільшення технологічного відриву провідних держав світу і нарощування їх можливостей щодо протидії створенню конкурентоспроможних російських інформаційних технологій;

• діяльність космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав;

• розробка низкою держав концепцій інформаційних війн, які передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн світу, порушення нормального функціонування інформаційних і телекомунікаційних систем, збереження інформаційних ресурсів, отримання несанкціонованого доступу до них.

До *внутрішних джерел* загроз інформаційної безпеки відносяться:

• недостатня економічна міць держави і недостатнє фінансування заходів щодо забезпечення інформаційної безпеки;

• критичний стан вітчизняних галузей промисловості;

• відставання від провідних країн світу за рівнем інформатизації всіх видів людської діяльності (державного управління, промисловості, кредитно-фінансової сфери, освіти, охорони здоров'я, сфери послуг та побуту громадян);

• недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика;

• несприятлива криміногенна обстановка, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері, отримання кримінальними структурами доступу до конфіденційної інформації, посилення впливу організованої злочинності на життя суспільства;

• недостатня координація діяльності щодо формування та реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки Російської Федерації;

• нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком інформаційного ринку Росії;

• зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки;

• недостатня активність федеральних органів державної влади, органів державної влади суб'єктів в інформуванні суспільства про свою діяльність, у роз'ясненні прийнятих рішень, у формуванні відкритих державних ресурсів і розвитку системи доступу до них громадян.

Література:

1. Інформаційні технології в юридичній діяльності під редакцією П.У Кузнецова.
2. Інформаційна безпека України в умовах євроінтеграції. Авторів В.А Лілкан, Ю.Е. Максименко, В.М. Желіховський.
3. Підручник - Забезпечення інформаційної безпеки держави.

Місевіч Катерина

Держаний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ

Управление доступом – это механизм безопасности, который управляет процессом взаимодействия пользователей с системами и ресурсами, а также систем между собой. Этот механизм защищает системы и ресурсы от несанкционированного доступа и принимает участие в определении уровня авторизации после успешного прохождения процедуры аутентификации. Нельзя забывать о том, что кроме пользователей, в сети существуют и другие сущности, которым нужен доступ к сетевым ресурсам и информации. В процессе управления доступом необходимо знать и понимать определения

субъекта и объекта. Доступ – это поток информации между субъектом и объектом. Субъект – активная сущность, запрашивающая доступ к объекту или данным внутри объекта. Субъектом может быть пользователь, программа или процесс, использующий доступ к объекту для выполнения своей задачи. Объект – пассивная сущность, содержащая информацию. Объектом может быть компьютер, база данных, файл, компьютерная программа, директория или поле таблицы базы данных. Например, если вы просматриваете информацию в базе данных, вы являетесь активным субъектом, а база данных – пассивным объектом. Рисунок 2-1 иллюстрирует субъекты и объекты.

Модель управления доступом – это структура, которая определяет порядок доступа субъектов к объектам. Для реализации правил и целей этой модели используются технологии управления доступом и механизмы безопасности.

Важно понимать основные характеристики трех моделей управления доступом:

- **DAC** – владельцы данных решают, кто имеет доступ к ресурсам. Политика безопасности реализуется с помощью ACL.
- **MAC** – политика безопасности реализуется операционной системой посредством меток безопасности.
- **RBAC** – решения о предоставлении доступа принимаются системой на основании ролей и/или должностей субъектов.

Система, которая использует ***дискреционное (избирательное) управление доступом*** (DAC – Discretionary Access Control) позволяет владельцу ресурса определять, какие субъекты могут использовать этот ресурс.

Эта модель называется дискреционной (избирательной), т.к. управление доступом основано на решениях владельца. Часто руководители подразделений являются владельцами данных в рамках своих подразделений. Будучи владельцами, они могут решать, кому следует, а кому не следует иметь доступ к этим данным. В модели DAC ограничения доступа основываются на авторизации пользователя. Это означает, что владельцы могут определять, какой тип доступа может быть разрешен к их объектам. Если компания использует модель DAC, сетевой администратор может разрешить владельцам ресурсов управлять доступом пользователей к своим ресурсам. Чаще всего модель DAC реализуется посредством списков контроля доступа (ACL), содержимое которых определено владельцами. Работа ACL реализуются средствами операционной системы. Это может позволить пользователям использовать информацию динамически вместо более статичного мандатного или ролевого управления доступом.

В модели ***мандатного управления доступом*** (MAC – Mandatory Access Control) пользователи и владельцы данных не могут самостоятельно определять, кто может иметь доступ к файлам. Окончательное решение принимает операционная система, и это решение может не совпадать с желаниями пользователя. Эта модель является более структурированной и жесткой, она основана на системе меток безопасности

(security label). Когда используется модель MAC, каждый субъект и объект должен иметь метку критичности, также называемую меткой безопасности. Эта метка указывает на классификацию и различные категории. Классификация указывает на уровень критичности, а с помощью категорий реализуется принцип «необходимо знать» (need-to-know). Классификация использует иерархическую структуру, в которой один уровень является более доверенным, чем другой.

Модель ***ролевого управления доступом*** (RBAC – Role-based Access Control), также называемая ***недискреционным управлением доступом*** (Nondiscretionary Access Control), использует централизованно администрируемый набор контролей, предназначенных для определения порядка взаимодействия субъекта с объектом. Этот тип модели разрешает доступ к ресурсам, основываясь на роли пользователя в компании. Это называют недискреционным подходом, поскольку назначение пользователю роли является неизбежным. Это означает, что если вам в компании назначена роль «Подрядчик», вы ничего с этим сделать не можете. Вы не определяете самостоятельно, какая роль вам будет назначена.

Ядро RBAC. Этот компонент должен быть интегрирован в каждую реализацию RBAC, т.к. это основа данной модели. Пользователи, роли, разрешения, операции и сессии определяются на основании политики безопасности.

Иерархии ролей определяют порядок наследования между ролями. Эта модель позволяет организовать разделение обязанностей(separation of duties).

- **Статическое разделение обязанностей** (SSD – Static Separation of Duty) **посредством RBAC.**

Это может использоваться для предотвращения мошенничества, предоставляя постоянный ограниченный набор привилегий (например, пользователь не может быть одновременно членом групп «Кассир» и «Контролер»).

- **Динамическое разделение обязанностей** (DSD – Dynamic Separation of Duties) **посредством RBAC**. Это может использоваться для предотвращения мошенничества, предоставляя ограничение набора возможных привилегий в рамках одной сессии. Это немного сложнее. Управление доступом в модели RBAC может происходить следующими способами:
- **Не-RBAC**. Назначение прав пользователям производится напрямую в приложениях, роли не используются.
- **Ограниченное RBAC**. Пользователям назначены несколько ролей, а также отдельные права в приложениях, которые не имеют функциональности ролевого управления доступом.
- **Гибридное RBAC**. Пользователям назначены роли, связанные с различными приложениями. Этим ролям назначены только выбранные права.
- **Полное RBAC**. Пользователям назначены корпоративные роли.

Литература: Руководство для подготовки к экзамену CISSP, Шон Харрис.

Чабан Богдан
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

АЛГОРИТМИ АСИМЕТРИЧНОГО ШИФРУВАННЯ ТА ЇХ ВИКОРИСТАННЯ ПІД ЧАС ЗАХИСТУ ІНФОРМАЦІЇ

Асиметричні алгоритми шифрування дозволяють забезпечувати шифрування інформації, що направляться йому необмеженою кількістю відправників. Крім того, використання цих алгоритмів дозволяє проводити автентифікацію учасників обміну інформацією та здійснювати контроль цілісності переданої інформації.

Загальний принцип роботи асиметричних алгоритмів полягає в наступному:

- учасник інформаційного обміну генерує пари ключів. При цьому дані, зашифровані одним із ключів, можуть бути розшифровані тільки іншим ключем. Один із цих ключів є відкритим (загальнодоступним), інший — закритим (секретним). Секретний ключ учасник зберігає в себе, а відкритий поширює всім бажаючої відправляти йому шифровані повідомлення. Відкритий ключ - це функція, за допомогою якої відправник може зашифрувати своє повідомлення, але ні він сам, ні хто-небудь інший не може дешифрувати це повідомлення, використовуючи відкритий ключ. Для дешифрування повідомлення (тобто здійснення зворотної операції — обчислення значення аргументу за значенням функції) необхідно знати деякий параметр зазначеної функції, що, по суті, і є закритим ключем;

- відправник повідомлення шифрує інформацію відкритим ключем і передає її одержувачеві по каналах зв'язку;

- одержувач дешифрує повідомлення, використовуючи свій закритий ключ.Найпоширеніші алгоритми асиметричного шифрування:

- RCA. Алгоритм розроблено в 1977 році. Використовує відкриті ключі, що забезпечують перетворення інформації «тільки в одну сторону» (шифрування) за рахунок фактори- зації (розкладання на множники) великих чисел;

- ECC (Elliptic Curve Cryptography). Односпрямованість перетворень (шифрування) забезпечується в цьому методі складністю математичних обчислень, пов'язаних з еліптичними кривими. Електронний цифровий підпис є електронним еквівалентом власноручного підпису. Він використовується не тільки для автентифікації відправника повідомлення, але й

для перевірки цілісності повідомлення. При використанні цифрового підпису для автентифікації відправника повідомлення застосовуються відкритий і закритий ключі. Процедура схожа на здійснювану в асиметричному шифруванні, але в цьому випадку закритий ключ служить для шифрування, а відкритий - для дешифрування. Алгоритм застосування електронного цифрового підпису складається з ряду операцій:

- генерується пара ключів: відкритий і закритий;
- відкритий ключ передається зацікавленій стороні (одержувачеві документів, підписаних стороною, яка сгенерувала ключі);
- відправник повідомлення шифрує його своїм закритим ключем і передає одержувачеві по каналах зв'язку;
- одержувач дешифрує повідомлення відкритим ключем відправника.

Суть у тім, що створити зашифроване повідомлення, при розшиф- ровці якого відкритим ключем виходить вихідний текст, може тільки власник закритого ключа, тобто відправник повідомлення. Використовувати для цього відкритий ключ неможливо.

Разом з електронним цифровим підписом звичайно застосовуються хеш-функції. Вони служать для того, щоб крім автентифікації відправника, яка забезпечується електронним цифровим підписом, гарантувати, що повідомлення не має перекручувань, і одержувач одержав саме те повідомлення, що підписав і відправив йому відправник.

Хеш-функція - це процедура обробки повідомлення, в результаті дії якої формується рядок символів (дайджест повідомлення) фіксованого розміру. Найменші зміни в тексті повідомлення приводять до зміни дайджесту при обробці повідомлення хеш-функцією. Таким чином, будь- які зміни, внесені в текст повідомлення, відіб'ються на дайджесті.

Алгоритм застосування хеш-функції:

- перед відправленням повідомлення обробляється за допомогою хеш-функції. В результаті отримують його стислий варіант (дайджест); саме повідомлення при цьому не змінюється;
- отриманий дайджест шифрується закритим ключем відправника (підписується електронним цифровим підписом) і пересилається одержувачу разом з повідомленням;
- одержувач розшифровує дайджест повідомлення відкритим ключем відправника;
- одержувач обробляє повідомлення тою ж хеш-функ- цією, що й відправник, і отримує його дайджест; якщо дайджест, надісланий відправником, і дайджест, отриманий в результаті обробки повідомлення одержувачем, збігаються, роблять висновок, що у повідомлення не було внесено змін.

Дереча Наталія
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Інформаційна безпека держави — це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

Відповідно до законодавства України поняття "інформаційна безпека" має таке визначення:*"стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації."*

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) по відношенню до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Поняття інформаційних технологій (ІТ) включає в себе широкий обсяг дисциплін і сфер діяльності і стосується технічних засобів обробки і передачі даних (чи інформації).

В англійській мові поняття безпеки ІТ має два значення. Поняття *функціональної безпеки* (англ. *safety*) означає, що система коректно і у повному обсязі реалізує *ті і лише ті* цілі, що відповідають намірам її власника, тобто функціонує відповідно до існуючих вимог. Поняття власне *інформаційної безпеки* (англ. *security*) стосується безпечності процесу технічної обробки інформації і є властивістю функціонально безпечної системи. Така система повинна унеможливлювати несанкціонований доступ до даних та запобігати їхній втраті у разі виникнення збоїв.

Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити

число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека — це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію (або дані) можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм.

Інформаційна безпека організації — цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інформаційна безпеки особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується модель CIA:

- Конфіденційність (англ. *confidentiality*) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем
- Цілісність (англ. *integrity*) — означає неможливість модифікації неавторизованим користувачем
- Доступність (англ. *availability*) — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Список використаної літератури

1. е-майбутнє та інформаційне право / [В. Брижко, В. Цимбалюк, Ю. Базанов]; за ред. доктора еко-номічних наук, професора, члена-кореспондента АПрН України М. Швеця. – [2-е вид., доп.]. – К. : НДЦПІ АПрН України, 2006. – 234 с.

2. Макаренко Є.А. Європейська інформаційна політика [Текст]: [монографія] / Є.А. Макаренко. – К.: Наша культура і наука, 2000. – 368 с.

3. Про Концепцію Національної програми інформатизації [Електронний ресурс]: Закон України: [від 04.02.1998 р. № 75/98-ВР]. – режим доступу: www.rada.gov.ua; www.bod.kiev.ua

Адамович Олексій
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

НАБІР ПРОТОКОЛІВ IPSec ДЛЯ СТВОРЕННЯ ЗАХИЩЕННОГО КАНАЛУ ЗВЯЗКУ МІЖ ДВОМА ПРИСТРОЯМИ У ВЕБ-СЕРЕДОВИЩІ

Набір протоколів **IPSec** (Internet Protocol Security) надає спосіб створення захищеного каналу для безпечного обміну даними між двома пристроями. Такими пристроями, що працюють через захищений канал, можуть бути два сервера, два маршрутизатора, робоча станція і сервер, два шлюзу між двома різними мережами. IPSec - це загальноприйнятий стандарт, що забезпечує захист на мережевому рівні. Він може бути більш гнучкий і менш доріг, в порівнянні з методами наскрізного і канального шифрування.

У IPSec застосовуються стійкі методи шифрування і аутентифікації. зазвичай він застосовується для створення VPN-тунелів між мережами через Інтернет, хоча може використовуватися і для створення комунікаційних тунелів між окремими комп'ютерами.

IPSec - це не жорсткий протокол, який диктує тип алгоритму, ключів і використовуваних методів аутентифікації. IPSec – це відкрита модульна платформа, що забезпечує більшу гнучкість для компаній, які обрали цю технологію. До складу IPSec входять два основні протоколи безпеки: **AH** (Authentication Header - Аутентифікація заголовка) і **ESP** (Encapsulating Security Payload - Безпечна інкапсуляція вмісту). AH - це протокол аутентифікації, а ESP - протокол аутентифікації і шифрування, використовуваний криптографічними механізмами для виконання аутентифікації джерела, а також забезпечення конфіденційності і цілісності повідомлень.

IPSec може працювати в одному з двох режимів: **транспортний режим**, в якому захищене вміст повідомлень, і **тунельний режим**, в якому захищене не тільки вміст повідомлень, а й заголовки пакетів, і інформація маршрутизації. При роботі ESP в транспортному режимі, він виконує шифрування тільки вмісту повідомлень, що в разі їх перехоплення не дозволить не уповноваженою особам прочитати інформацію. тунельний режим забезпечує більш високий рівень захисту, додатково шифруючи заголовки і закінчення пакетів даних, в яких атакуючий може знайти корисні для нього відомості.

Кожен пристрій має мати одну або більше **асоціацій безпеки** (SA – security association) на кожне використовуване їм безпечне з'єднання. SA - це конфігураційна запис в налаштуваннях пристрою, необхідна для роботи з'єднання IPSec. SA грає одну з найважливіших ролей в архітектурі IPSec. Коли два пристрої завершили процес «рукостискання», в рамках якого вони досягли угоди по великій кількості різних комунікаційних параметрів, ці параметри повинні бути десь збережені. Саме для цього і потрібна SA. SA може містити

ключі аутентифікації і шифрування, інформацію про узгоджених алгоритмах, термін життя ключа, IP-адреса відправника. Якщо отримано пакет за допомогою протоколу IPSec, саме SA каже пристрою, що потрібно робити з цим пакетом. Так, якщо пристрій Б отримує пакет від пристрою В за допомогою IPSec, пристрій Б має подивитися в відповідну SA, щоб дізнатися, як розшифрувати пакет, як правильно аутентифицировать відправника пакета, який ключ використовувати, як відповідати на повідомлення при необхідності.

SA враховує тільки один напрямок передачі даних, тому пристрій повинен мати для кожного окремого комунікаційного каналу одну SA для вихідного трафіку і одну - для вхідного. Таким чином, якщо пристрій підключено до трьох інших пристроїв, воно повинно мати не менше шести SA - по дві (одна для вихідного трафіку, інша – для вхідного) на кожне віддалене пристрій. Яким чином пристрої зберігають SA і забезпечують застосування потрібних SA для відповідних з'єднань? Це здійснюється з допомогою **індексів параметрів безпеки** (SPI - security parameter index). На кожному пристрої є SPI, який відстежує різні SA і повідомляє влаштуванню, який йому потрібен SA для обробки того чи іншого пакета. Значення SPI вказується в заголовку пакета IPSec, пристрій зчитує це значення, щоб знайти потрібний SA.

Оскільки IPSec є платформою, він не диктує конкретні алгоритми хешування і шифрування або процедури обміну ключами. Управління ключами може виконуватися вручну або автоматично з використанням протоколу управління ключами. Стандартом «де-факто »для IPSec є використання IKE (Internet Key Exchange - Обмін ключами в Інтернет), який є комбінацією протоколів ISAKMP і OAKLEY. **ISAKMP** (Internet Security Association and Key Management Protocol - Протокол управління ключами і асоціаціями безпеки в Інтернет) - це архітектура обміну ключами, незалежна від типу використовуваних механізмів, пов'язаних з ключами. ISAKMP надає платформу, угоду про деталі використання якої досягається в процесі створення з'єднання IPSec (алгоритми, протоколи, режими, ключі). Протокол OAKLEY - це протокол, який якраз і реалізує досягнення цього угоди.

IPSec з усіма цими компонентами і різними можливими конфігураціями дуже різноманітний. Це різноманіття забезпечує високу ступінь гнучкості, оскільки компанія має великий вибір конфігурацій для досягнення необхідного їй рівня захисту.

Література:

1.https://uk.wikipedia.org/wiki/IPsec
2.“A Cryptographic Evaluation of IPSec,” by N. Ferguson and Bruce Schneier www.schneier.com/paper-ipsec.html
3. “An Introduction to IP Security (IPSec) Encryption,” Cisco Systems, Inc. www.cisco.com/warp/public/105/IPSECpart1.html

Сокол Антон
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Швидкий розвиток мереж і їх об'єднання в мережу Інтернет призвів до зростання числа порушень принципів інформаційної безпеки. Аналіз останніх досліджень показав, що основним недоліком переважної кількості сучасних комерційних систем виявлення атак є низька, близька до нуля, ефективність виявлення невідомих атак. Розуміння природи аномалій трафіку у мережі є актуальним питанням. Незалежно від того, шкідливими чи ні є аномалії, важливо проаналізувати їх з двох причин: – аномалії можуть створювати перевантаження в мережі і підвищити використання ресурсів маршрутизаторів, що робить виявлення цих аномалій вкрай важливим; – деякі аномалії не обов'язково впливають на мережу, але вони можуть мати серйозний вплив на клієнта або кінцевого користувача. Проведемо класифікацію методів виявлення аномалій мережевого трафіку. Кластерний аналіз. Суть даної групи методів полягає в розбитті множини спостережуваних векторів-властивостей системи на кластери, серед яких виділяють кластери нормальної поведінки.

Статистичний аналіз. Дана група методів використовує побудову статистичного профілю поведінки системи протягом деякого періоду «навчання», при якому поведінка системи вважається нормальною. Нейронні мережі. Нейронні мережі для виявлення аномалій навчаються протягом деякого періоду часу, коли вся спостережувана поведінка вважається нормальною. Експертні системи. Інформація про нормальну поведінку представляється в подібних системах у вигляді правил, а спостережувана поведінка у вигляді фактів. Імунні мережі. Виявлення аномалій є одним з можливих додатків імунних методів. Так як кількість прикладів нормальної поведінки звичайно на порядок перевищує число прикладів атак, використання імунних мереж для виявлення аномалій має велику обчислювальну складність. Розглянемо методи виявлення аномалій мережевого трафіку, що використовують нейронні мережі та математичний апарат вейвлет-аналізу більш детально.

Штучна нейронна мережа (ШНМ) є математичною (а також програмною або апаратною) моделлю, побудованою за принципом організації та функціонування біологічних нейронних мереж. Сьогодні існує кілька архітектур штучних нейронних мереж, які з успіхом застосовуються для вирішення складних технічних і економічних завдань. Деякими з особливостей ШНМ є здатність в процесі навчання виявляти складні залежності між вхідною і вихідною інформацією. Нейронні мережі мають ряд переваг, які вигідно відрізняють їх від традиційних рішень, а саме високу ступінь паралелізму обробки інформації; здатність до узагальнення; адаптацію до змін

навколишнього середовища; розпізнавання зашумлених образів; низький рівень ресурсоємності. Для виявлення аномалій мережевого трафіку можна використати метод на основі кореляційного аналізу IP-адрес призначення вихідного трафіку на виході маршрутизатора. Для ефективного виявлення аномалій за допомогою статистичного аналізу кореляція адресних даних здійснюється за допомогою дискретного вейвлет- перетворення. Спочатку обчислюється кількість рівнів вейвлет-розкладу сигналу як двійковий логарифм від кількості розбиттів сигналу. Потім обчислюються початкові значення апроксимуючих коефіцієнтів, використовуючи значення трафіку, що були записані в масиві і викликається підпрограма вейвлет-перетворення Хаара, яка обчислює апроксимуючі та деталізуючи коефіцієнти різних рівнів розкладу мережевого трафіку. Далі здійснюється зворотне вейвлет-перетворення, за допомогою якого відбувається реконструкція сигналу, а також визначення аномальної і трендової складової сигналу. Значення аномальної складової дозволяє встановити наявність атаки на комп'ютерну мережу. З проведеного дослідження можна зробити висновок, що використання вейвлет- аналізу для виявлення атак на комп'ютерну мережу вимагає меншого часу, ніж нейронних мереж, проте останні, за рахунок можливості навчання, дозволяють виявити всі відомі атаки.

Література:

Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / Соколов А.В., Шаньгин В.Ф. – М. : ДМК Пресс, 2002 – 656 с.

Куссуль Н.Н. Нейросетевая модель пользователей компьютерных систем / Куссуль Н.Н., Сидоренко А.В., Скакун С.В. // Кибернетика и вычислительная техника. – 2004.

Петухов А.П. Введение в теорию базисов всплесков / А.П. Петухов. – СПб.: Изд- во СПбГТУ, – 1999. – 132 с.

Боцюк Остап
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КАТЕГОРИИ АТАК

Во время работы компьютерных систем часто возникают различные проблемы. Некоторые – по чьей-то оплошности, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится ущерб. Поэтому будем называть такие события атаками, независимо от причин их возникновения.

Существуют четыре основных категории атак:

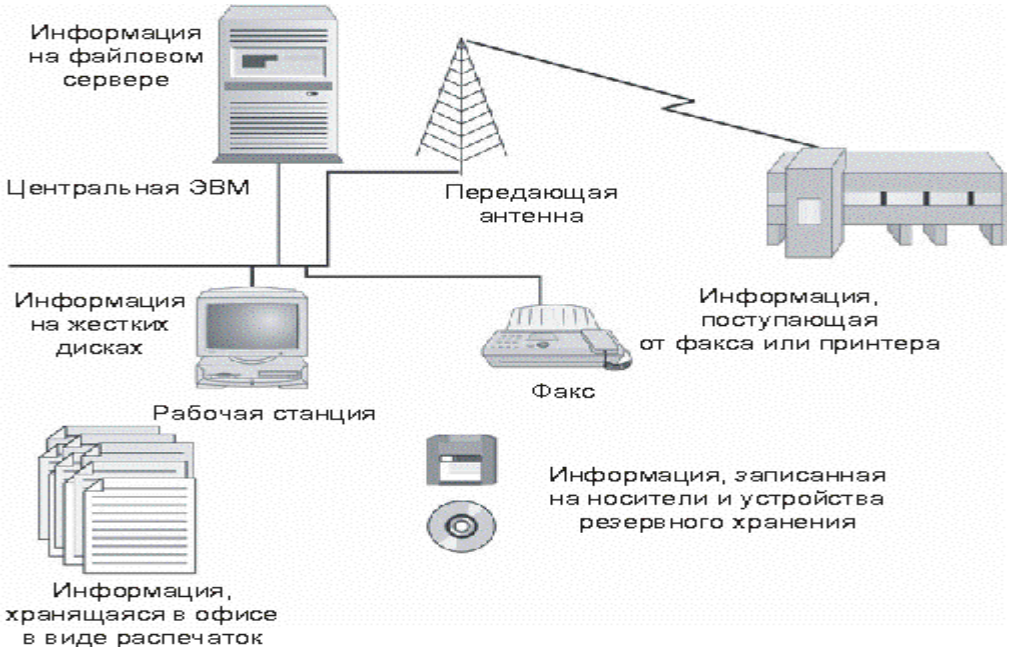
1. Атаки доступа.

2. Атаки модификации.
3. Атаки на отказ в обслуживании.
4. Атаки на отказ от обязательств.

Определение атаки доступа

Атака доступа – это попытка получения информации злоумышленником, для просмотра которой у него нет разрешений, и которая направлена на нарушение конфиденциальности информации. Для осуществления данной атаки необходима информация и средства для ее передачи.

Рис. 1. Атака доступа возможна везде, где существуют информация и средства для ее передачи



К атакам доступа можно так же отнести подсматривание, подслушивание и перехват.

- Подсматривание – это просмотр файлов или документов для поиска интересующей злоумышленника информации.
- Подслушивание – когда кто-то слушает разговор, участником которого он не является (часто при этом он использует электронные устройства).
- Перехват – захват информации в процессе ее передачи к месту назначения.

Прежде, чем разобраться, как выполняются атаки доступа, давайте разберемся, где хранится информация в электронном виде.

А хранится она:

- на рабочих станциях;
- на серверах;
- в портативных компьютерах;

- на флоппи-дисках;
- на компакт-дисках;
- на резервных магнитных лентах.

Последние четыре пункта мы рассматривать не будем, т.к. злоумышленник может их просто украсть. С первыми двумя дело обстоит иначе. При легальном доступе к системе злоумышленник будет анализировать файлы, просто открывая один за другим. При несанкционированном доступе, взломщик постарается обойти систему контроля и получить доступ к нужной информации. Сделать это не сложно. Необходимо установить в компьютерной системе сетевой анализатор пакетов (sniffer). Для этого взломщик должен повысить свои полномочия в системе или подключиться к сети. Анализатор настроен на захват любой информации, проходящей по сети, но особенно – на пользовательские идентификаторы и пароли.

Подслушивание выполняется и в глобальных компьютерных сетях типа выделенных линий и телефонных соединений. Однако такой тип перехвата требует наличия соответствующей аппаратуры и специальных знаний. В этом случае наиболее удачным местом для размещения подслушивающего устройства является шкаф с электропроводкой.

А с помощью специального оборудования квалифицированный взломщик может осуществить перехват в системах оптико-волоконной связи. Однако, что бы добиться успеха, он должен поместить свою систему в линии передачи между отправителем и получателем информации. В интернете это выполняется посредством изменения разрешения имени, в результате чего имя компьютера преобразуется в неправильный адрес. Трафик перенаправляется к системе атакующего вместо реального узла назначения. При соответствующей настройке такой системы отправитель так и не узнает, что его информация не дошла до получателя.

Определение атаки модификации

Атака модификации – это попытка неправомерного изменения информации. Она направлена на нарушение целостности информации и возможна везде, где существует или передается информация.

Существует три вида атаки модификации – это замена, добавление и удаление.

- Замена – замена существующей информации направлена как против секретной, так и общедоступной информации.
- Атака добавления – добавление новых данных.
- Атака удаления означает перемещение существующих данных.

Все три вида атаки модификации используют уязвимые места систем, например, «бреши» в безопасности сервера, позволяющие заменить домашнюю

страницу. И даже в этом случае необходимо основательно поработать во всей системе, чтобы воспрепятствовать обнаружению. Т.к. транзакции нумеруются последовательно, и удаление или добавление неправильных операционных номеров будет замечено.

В случае, если атака модификации производится при передаче информации, то необходимо сначала выполнить перехват интересующего трафика, а затем внести изменения в информацию перед ее отправкой к пункту назначения.

Атаки на отказ в обслуживании

Атаки на отказ в обслуживании (Denial-of-service, DoS) – это атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров. Другими словами, эта атака «Вандализм», т.к. злоумышленник В результате DoS-атаки обычно не получает доступа к компьютерной системе и не может оперировать с информацией.

- DoS-атака, направленная против информации – уничтожает, искажает или переносит в недоступное место последнюю.
- DoS-атака, направленная на приложения, обрабатывающие или отображающие информацию, или на компьютерную систему, в которой эти приложения выполняются – делают невозможным решение задач, выполняемых с помощью такого приложения.
- Общий тип DoS-атак (отказ в доступе к системе) ставит своей целью вывести из строя компьютерные системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становится недоступной.
- Отказ в доступе к средствам связи заключается в выведении из строя средств связи, которые лишают доступ к компьютерным системам и информации.
- DoS-атаки, нацеленные непосредственно на компьютерную систему, реализуются через эксплоиты, использующие уязвимые места операционных систем или межсетевых протоколов. С помощью этих «брешей» атакующий посылает в приложение определенный набор команд, который оно не в состоянии правильно обработать, в результате чего приложение выходит из строя. Перезагрузка восстанавливает его работоспособность, но на время перезагрузки работать с приложением становится невозможно.

Определение атаки на отказ от обязательств

Атака на отказ от обязательств направлена против возможности идентификации информации, или дать неверную информацию о реальном событии либо транзакции.

К данному виду атаки относятся:

- Маскарад – это выполнение действий под видом другого пользователя или другой системы.
- Отрицание события – это отказ от факта совершения операции.

• DoS-атаки против интернета – это атака на серверы корневых имен интернета.

Рухлядко Михайло
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

СТАН ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ НА 2016 РІК

На порядку денному України постали завдання переходу до нового етапу розвитку суспільства, наступного за постіндустріальним – етапу Інформаційного суспільства, головним змістом якого є діяльність людей, що пов’язана з отриманням, обробкою та створенням інформації. Сучасний стан захищеності інформаційних систем об'єктів критичної інфраструктури (і критичної інформаційної інфраструктури, як її підмножини) на сьогодні є не задовільним для України. Внаслідок сильної зв'язності інформаційного суспільства стан захисту об'єктів критичної інфраструктури України прямо та опосередковано впливає на інші країни і все більше впливає на імідж України в світовому інформаційному просторі.

Аналіз чинної законодавчої бази у сфері інформаційної безпеки вказує на те, що на сьогодні в умовах проведення широкомасштабних інформаційних атак на українське суспільство відсутні концептуальні документи у зазначеній сфері, оскільки відповідно до Рішення РНБО України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», введеним в дію Указом Президента № 449/2014 від 01.05.2014 скасовано Доктрину інформаційної безпеки України № 514/2009 від 08.07.2009 року та передбачено розробку низки законодавчих актів, зокрема, Стратегії розвитку інформаційного простору України, Стратегії кібернетичної безпеки України, проекту Закону України про кібернетичну безпеку України. Разом з тим, на сьогодні жодного із зазначених актів не прийнято.

На сьогодні в Україні тими чи іншими аспектами забезпечення інформаційної безпеки займаються різні державні органи та установи, серед яких – Національна рада України з питань телебачення і радіомовлення, Держкомтелерадіо України, Служба безпеки України, Держспецзв’язку України, Служба зовнішньої розвідки України, Міністерство оборони України, МВС України, Міністерство закордонних справ України, Міністерство культури України, Міністерство юстиції України,та інші, діяльність яких часто дублюється та не координується.

Найбільш актуальними для України на сьогодні є наступні загрози:

-можливість ураження інформаційних систем об’єктів критичної інфраструктури (у сфері енергетики, телекомунікацій, фінансово-банківського сектора, транспорту та оборони);

-високий рівень кіберзлочинності, що має транснаціональний характер;

-діяльність іноземних спецслужб та розвідувальних служб інших країн, хакерських угруповань;

-поширення негативного іміджу України, що обумовлюється низьким рівнем соціально-економічного розвитку, корумпованістю та недієвістю органів державної влади, складною криміногенною ситуацією та незадовільним для українців рівнем надання соціальних сервісів українським державним апаратом;

-вкрай низька ефективність правоохоронних органів, силових відомств, державних органів при протидії комп’ютерним атакам (кіберагресії);

-не ефективна та не гнучка система управління національним сегментом мережі Інтернет, доменним простором .ua та .УКР;

-не прозора та не дієва схема взаємодії держави і громадян у питаннях кібербезпеки.

Відповідно до законодавства питання протидії зовнішнім та внутрішнім кіберзагрозам в Україні належать до компетенції Адміністрації Державної служби спеціального зв’язку та захисту інформації України, Служби безпеки України, Міністерства внутрішніх справ України. До зазначеної діяльності також залучаються Міністерство оборони України та інші центральні органи виконавчої влади.

Фактичний стан захищеності України в інформаційному плані не дозволяє ефективно захищати, розвивати її телекомунікаційну складову, що вкрай негативно впливає на внутрішню та зовнішню політику України, уповільнює економічний та соціальний розвиток.

Для забезпечення координації діяльності суб’єктів кібернетичної безпеки, враховуючи власний досвід України та сучасні кращі закордонні практики, найближчим часом необхідне створення Національного центру кібернетичної безпеки, до складу якого увійдуть:

-Оперативна рада (група) кібербезпеки – створена відповідно до наказу Адміністрації Держспецв’язку, повинна включати адміністративні контакти (керівників ключових підрозділів держави і приватного секторів, зокрема операторів/провайдерів ринку телекомунікацій), мати дорадчий та консультативний статус, брати участь у організації важливих для держави подій в частині що стосується;

-Центр боротьби з кіберзлочинністю та розслідувань – створений на базі Держспецзв’язку, повинен включати співробітників УБК МВС України, ДКЗІДСІБ СБ України, МО України та СЗР України. Центр з боротьби з кіберзлочинністю та розслідувань мати права суб’єкту регулювання ринку телекомунікацій, правоохоронного органу та криміналістичної лабораторії з комп’ютерної тематики:

-право на досудове блокування інформаційних ресурсів з наступних причин: екстремізм, тероризм, розпалювання міжнаціональної та міжконфесійної ворожнечі і масові заворушення, дитяча порнографія тощо;право визначення підслідності, відкриття і закриття кримінального провадження, слідчі дії, робота з НКП;криміналістичних експертиз (право залучати експертів).

-Співробітники Центру з боротьби з кіберзлочинністю та розслідувань повинні бути штатними співробітниками правоохоронних органів, у компетенції яких лежить боротьба з кіберзагрозами. У межах Центру з боротьби з кіберзлочинністю та розслідувань вони виконують свої прямі завдання та користуються правовим полем цих міністерств, координуючи свою діяльність за допомогою Оперативної ради (групи) кібербезпеки та за допомогою підрозділу з визначення підслідності.

-Центр моніторингу та технічного супроводження системи захисту державних інформаційних ресурсів у складі:відділ антивірусного захисту інформації – антивірусний захист держави, вивчення та розробка нових зразків ШПЗ;

-відділ CERT-UA – реагування на інциденти інформаційної безпеки, досудове вирішення спорів, надання допомоги громадянам, міжнародна діяльність;відділ аудиту інформаційної безпеки та оцінок стану захищеності – права інспектування, оцінок стану захищеності ДІР в ІТС ОДВ, право накладання штрафу за адмінпорушення у сфері захисту інформації і подання заявок до Центру з боротьби з кіберзлочинністю та розслідувань (пп. 2.1-2.3);

-відділ стандартів та внутрішнього контролю – експертизи ТЗІ та КЗІ, розробка та впровадження стандартів з ІБ для потреб суб'єктів кібернетичної безпеки, аналітична робота з питань кібербезпеки, контроль ефективності роботи з основних завдань Національного центру кібернетичної безпеки, винесення пропозицій на розгляд Оперативної ради (групи) кібербезпеки;

-відділ технічних засобів та МТЗ – закупівля МТЗ та техніки, ведення господарської діяльності, тестування нових розробок у галузі телекомунікацій тощо;

-відділ технічного супроводження системи захисту державних інформаційних ресурсів – адміністрування СЗДІ, надання телекомунікаційних сервісів та сервісів з кіберзахисту від імені Національного центру кібернетичної безпеки для суб'єктів кібернетичної безпеки.

Усі співробітники Національного центру кібернетичної безпеки повинні бути громадянами і патріотами України, володіти державною мовою. Повинно бути реалізовано механізм усунення будь-якого співробітника Національного центру кібернетичної безпеки за рішенням Оперативної ради (групи) кібербезпеки з наслідком у вигляді неможливості заняття посад у державному апараті на деякий тривалий час (за поданням відділу внутрішньої безпеки та аудиту та керівника підрозділу). Це повинно обов'язково висвітлюватись у ЗМІ відділом взаємодії з ЗМІ на відповідному публічному веб-ресурсі у мережі

Інтернет (на початковому етапі це може бути веб-сайт CERT-UA – www.cert.gov.ua).З метою протидії корупції необхідно належне фінансове забезпечення усіх співробітників Національного центру кібернетичної безпеки на рівні, вищому ніж у аналогічних підрозділах суб'єктів кібернетичної безпеки України (повинен бути реальний попит на кожне місце та конкурсний відбір на кожну посаду). Це значно ускладнить деструктивний вплив спецслужб інших країн на роботу Національного центру кібернетичної безпеки, а також уповільнить відтік висококваліфікованих кадрів.

Висновок: на даний момент Україна є в поганому становищі з огляду інформаційної і кібернетичної безпеки,проте має багато переспектив та можливостей розвитку в цій сфері,адже з'являються нові шляхи захисту і нові працівники у цьому напрямі.

Література:

1.http://stratcom.co.ua/shhodo-okremih-organizatsijno-pravovih-pitan-zabezpechennya-informatsijnoyi-bezpeki-ukrayini/

2. http://cert-ua.livejournal.com/12036.html

Платоненко Артем Вадимович
Державний університет телекомунікацій,
Навчально-науковий інститут захисту інформації
кафедра Систем технічного захисту інформації
м.Київ

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ КОРИСТУВАЧІВ СУЧАСНИХ МОБІЛЬНИХ ПРИСТРОЇВ В УКРАЇНІ

Розглянуто вразливості сучасних мобільних пристроїв з використанням високошвидкісних мобільних мереж, адже кожен третій житель України має смартфон з сенсорним екраном, а висока швидкість передачі даних є зручною не тільки для користувача, а і для зловмисника, що несе за собою небезпеку для інформації, яка зберігається та передається з використанням мобільних пристроїв.

Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається [1]. Швидкість передачі даних у мережах 4G, яка може досягати до 1 Гбіт/с (в 6 разів більше у порівнянні з найшвидшими мережами 3G), а в мережах 5G швидкість передачі даних може досягати до 5 Гбіт/с (в 80 разів більше ніж заявлена максимально можлива швидкість в мережах 3G-операторів України).

З використанням високошвидкісних мобільних мереж нового покоління, загрози інформаційної безпеки для державних та приватних установ [2] збільшуються, адже для зловмисників відкриваються більші технічні

можливості, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи, а не тільки для спілкування.

Кожен третій житель України (33%) має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – половина (50%). Порівняно з 2015 роком простежується зростання частки таких людей – з 26% до 33% у випадку загального населення і з 41% до 50% у випадку осіб до 50 років. Якщо серед молоді 65% користуються смартфонами, то серед осіб літнього віку – 5%. Типовий користувач смартфонів – це молода особа не старше 40 років з вищою освітою, яка проживає у середніх і великих містах України. Більшість (66%) користуються операційною системою Android, а 68% користувачів смартфонів мають досвід встановлення додатків. Найбільш популярними є соціальні мережі (73%), ігри (61%), навігація (51%), месенджери (49%) [3].

Нажаль неуважні або недосвідчені користувачі мобільних пристроїв встановлюють і зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисник може отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, його можливості збільшуються в рази.

Рівень розкриття кіберзлочинів в Україні становить в середньому 50%, при цьому 80% постраждалим вдається відшкодувати збитки, яких вони зазнали внаслідок дій злочинців. За даними опитування у якому взяли участь 502 експерта в області інформаційної безпеки та IT-фахівців, в рамках форуму Cisco «Технології кібербезпеки», у найближчі три роки інформаційна безпека матиме найбільший вплив на IT-стратегію компаній.

Основною перешкодою для захисту компаній від кіберзагроз 65,1% вважають дефіцит бюджету, 47% - брак фахівців з IT-безпеки.

- Основні загрози інформаційній безпеці організацій несуть забезпечення мобільності співробітників (50,4%) та Інтернет речей (20,5%);
- 4,2% організацій на сьогодні захищені максимально надійно;
- 49,7% - фахівців оцінюють захист на три бали з можливих п'яти.

Більше половини опитаних за останній рік мали проблеми з атаками, а саме: зараження шкідливим ПЗ - (70,2%), спам, фішинг і різні види інтернет-шахрайства (52,5%), DOS-атаки (37,4%), шпигунські атаки (20%), програми-вимагачі (18, 5%), спрямовані атаки хакерів (15,1%) і ботнети (12,5%).

Більша кількість компаній виявляють проблему протягом одного дня (37,3%). Протягом години це вдається зробити в 11,5% організацій, близько тижня потрібно для 31,5% фірм. Іншим компаніям потрібно більше часу.

Збиток, нанесений в результаті кібератаки, виражається переважно в збої системи (58,4%), втрата даних і неавторизований доступ до них також поширені: 25,2% і 14,9% відповідно. Крім того, в результаті дій зловмисників

фахівці втрачали час, не могли скористатися необхідним обладнанням, втрачали доступ до зашифрованих зловмисниками даних, несли репутаційні втрати [4].

В свою чергу, кількість сім-карт на ринку України продовжує зменшуватись, незважаючи на продаж великої кількості смартфонів на дві сім-картки
(більше 90%) можна зробити висновок, що користувачі стали більше приділяти увагу економії у використанні ресурсів мережі та більш сумлінно відноситись до можливостей своїх пристроїв. Таким чином, це можна вважати певним обмеженням для зловмисників, хоча і не суттєвим.

Враховуючи розвиток та поширення сучасних мобільних пристроїв, зростання їх апаратних можливостей, а також швидкості передачі даних в мережах мобільного зв'язку, для більш ефективного захисту треба бути уважнішим, використовувати перевірене програмне забезпечення, різні паролі для облікових записів, блокування пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати.

Одним із варіантів вирішення проблем інформаційної безпеки є NGFW (Next Generation Firewall – мережеві екрани нового покоління), використання яких набуває все більшого поширення, адже завдяки ним можливо обмежити трафік по категоріям та відслідковувати поведінку користувачів, надати доступ необхідним пристроям до певних сайтів, файлів, програм та оцінити можливі ризики від них.

Використовуючи таке програмно-апаратне забезпечення є можливість захистити корпоративну мережу від зловмисних дій, які могли б понести за собою значні збитки, а правильне налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв.

Література:

1. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах/ А. В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р.

2. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко, Київ, ДУТ, Сучасний захист інформації. Науковий журнал. – 2015. – № 4, с. 86 – 90.

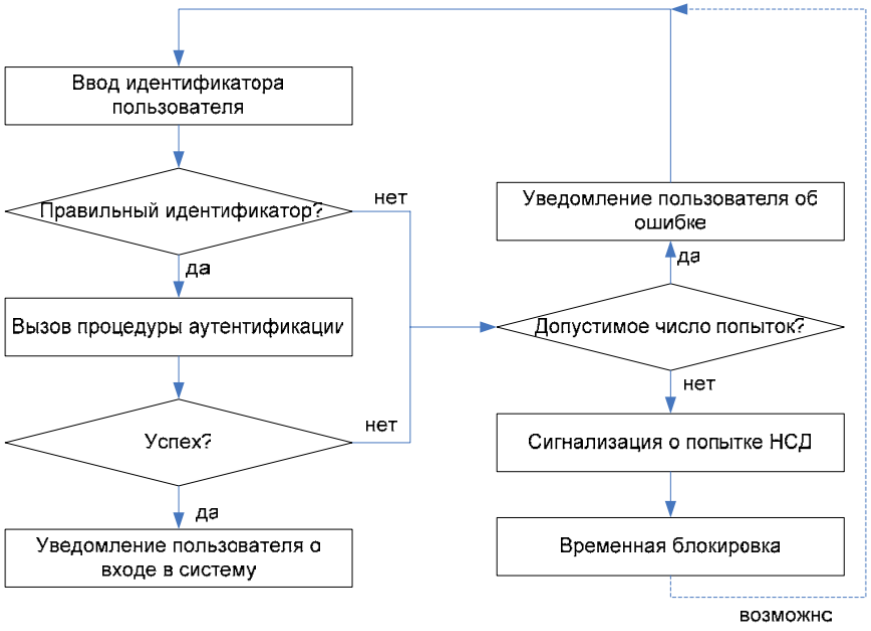
3. Використання смартфонів в Україні [Електронний ресурс] – Режим доступу: http://lead9.com/slide/slide.pdf

4. Cisco исследовала основные тенденции в сфере информационной безопасности на украинском рынке [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153526

Герега Ілля
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ. МЕТОДЫ АУТЕНТИФИКАЦИИ

Под ***идентификацией*** принято понимать присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных. В свою очередь, ***аутентификаци***я понимается как проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Тем самым, задача идентификации – ответить на вопрос «кто это?», а аутентификации - «а он ли это на самом деле?».



Базовая схема идентификации и аутентификации

Приведённая схема учитывает возможные ошибки оператора при проведении процедуры аутентификации: если аутентификация не выполнена, но допустимое число попыток не превышено, пользователю предлагается пройти процедуру идентификации и аутентификации еще раз.

Всё множество использующих в настоящее время методов аутентификации можно разделить на 4 большие группы:

1.Методы, основанные на знании некоторой секретной информации.

Классическим примером таких методов является парольная защита, когда в качестве средства аутентификации пользователю предлагается ввести пароль

– некоторую последовательность символов. Данные методы аутентификации являются наиболее распространёнными.

2.Методы, основанные на использовании уникального предмета.

В качестве такого предмета могут быть использованы смарт-карта, токен, электронный ключ и т.д.

3.Методы, основанные на использовании биометрических характеристик человека.

На практике чаще всего используются одна или несколько из следующих биометрических характеристик:

- отпечатки пальцев;
- рисунок сетчатки или радужной оболочки глаза;
- тепловой рисунок кисти руки;
- фотография или тепловой рисунок лица;
- почерк (роспись);
- голос.

Наибольшее распространение получили сканеры отпечатков пальцев и рисунков сетчатки и радужной оболочки глаза.

4.Методы, основанные на информации, ассоциированной с пользователем.

Примером такой информации могут служить координаты пользователя, определяемые при помощи GPS. Данный подход вряд ли может быть использован в качестве единственного механизма аутентификации, однако вполне допустим в качестве одного из нескольких совместно используемых механизмов.

Широко распространена практика совместного использования нескольких из перечисленных выше механизмов – в таких случаях говорят о ***многофакторной аутентификации***

Особенности парольных систем аутентификации

При всём многообразии существующих механизмов аутентификации, наиболее распространённым из них остаётся парольная защита. Для этого есть несколько причин, из которых мы отметим следующие:

- Относительная простота реализации.

Действительно, реализация механизма парольной защиты обычно не требует привлечения дополнительных аппаратных средств.

- Традиционность.

Механизмы парольной защиты являются привычными для большинства пользователей автоматизированных систем и не вызывают психологического отторжения – в отличие, например, от сканеров рисунка сетчатки глаза.

В то же время для парольных систем защиты характерен парадокс, затрудняющий их эффективную реализацию: стойкие пароли мало пригодны для использования человеком. Действительно, стойкость пароля возникает по мере его усложнения; но чем сложнее пароль, тем труднее его запомнить, и у пользователя появляется искушение записать неудобный пароль, что создаёт дополнительные каналы для его дискредитации.

Холод Богдан Вадимович
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ

В епоху процесів глобалізації засоби масової інформації впевнено посіли чільне місце серед засобів комунікації. Сама глобалізація як явище не була б можливою без діяльності сучасних електронних засобів комунікації та мас-медіа, які охоплюють усю планету.

ЗМІ відіграють чи не найголовнішу роль у сучасному політичному житті більшості держав. Вони виступають основним суб'єктом формування в суспільстві громадської думки про події та явища, що відбуваються в світі та в кожній окремо взятій країні. При цьому спостерігається зворотна закономірність: чим більш розвинутою є інформаційна мережа держави, тим менше залишається можливостей для використання інформації на користь якогось одного суб'єкта, і навпаки - при менш розвинутій мережі існує більше можливостей для її монополізації та подачі інформації у спотвореному або неповному вигляді.

Разом з тим проведене узагальнення вітчизняного досвіду свідчить про те, що в останні роки засоби масової інформації швидше були знаряддям політичної й економічної боротьби, аніж об'єктивно висвітлювали факти. Вони стали основною ареною, на якій розгортаються баталії між економічними й бюрократичними кланами, різноманітні сюжети про які добре продаються й користуються попитом. Вітчизняна ділова еліта усвідомила могутність ЗМІ, а також те, що політична рентабельність серйозних вкладень у них може мати корисні економічні наслідки.

З огляду на це недостатня увага з боку органів державної влади, громадських організацій і журналістів до проблем недостатнього правового врегулювання статусу ЗМІ, їх тотальної комерціалізації та монополізації, диктату власників ЗМІ та неефективного впливу на їх редакційну політику з боку держави може призвести до ситуації, коли маніпулювання суспільною свідомістю стане основною функцією вітчизняних засобів масової інформації. В такому випадку ЗМІ можуть стати знаряддями масової пропаганди й агітації, за допомогою яких ті чи інші особи або групи осіб будуть формувати громадську думку, тобто інструментом боротьби між ними. В свою чергу, це викличе істотну деформацію демократичної системи суспільства, наслідком якої стане подальше розростання низки негативних явищ - тіньової економіки, організованої злочинності, корупції, встановлення влади "сильної руки", виникнення інформаційної залежності від іноземних суб'єктів тощо через брак у вітчизняних ЗМІ повної та об'єктивної інформації.

В умовах існування альтернативних каналів інформації сучасні ЗМІ повинні мати приблизно однаковий потенціал впливу на громадськість (популярність, рівень довіри тощо). У такому випадку не буде мати значення кількість іноземних інформаційних компаній, які працюють на території держави, - їх вплив буде адекватно врівноважений діяльністю вітчизняних. І навпаки, при малопотужних вітчизняних інформаційних ресурсах існує можливість повної інформаційної ізоляції цілих регіонів чи навіть держав завдяки діяльності іноземних ЗМІ.

Найчастіше правом висвітлення подій для світової громадськості володіють американська CNN та британська ВПС (вторгнення військ США у Панаму в грудні 1989 р. - січні 1990 р., операція багатонаціональних сил "Буря в пустелі" в Кувейті та Іраку в 1991 році, вторгнення військ США на Гаїті у 1994 році, операції сил НАТО проти Югославії в 1999 році, Афганістану в 2001 році та Іраку в 2003 році).

Під час Оксамитової революції в листопаді 2003 р. у Грузії події у Тбілісі були під постійною увагою грузинських та (що відіграло особливу роль) закордонних ЗМІ. Так, 22 листопада 2003 р., удень, коли було силою захоплено Парламент Грузії, американська телекомпанія CNN вела прямий п'ятигодинний репортаж з місця подій.

Слід врахувати, що Грузія не володіє власними потужними рейтинговими ЗМІ, які могли б скласти конкуренцію світовим медіа-гігантам. Тому така прискіплива увага світової спільноти до перетворень на Північному Кавказі мала подвійне значення.

З одного боку, вона була фактором, що дозволив уникнути кровопролиття: опозиційні сили відчували зовнішню підтримку, оскільки кожен їх крок фіксувався на плівку, а захисники президента Шеварднадзе також не наважилися вдатися до силових засобів, оскільки це могло бути розцінено як розправа над неозброєним народом, тобто як злочин. При цьому всі учасники подій чудово пам'ятали судовий процес над Слободаном Мілошевичем у Гаазі, якого було звинувачено у злочинах проти людства.

З іншого боку, чи не були події у Грузії хрестоматійним прикладом проведення спеціальної інформаційної операції із широким застосуванням можливостей ЗМІ та щедро фінансованих із-за кордону неурядових організацій? Сьогодні можемо будувати будь-які версії, але в будь-якому випадку маємо яскравий приклад наслідків недорозвиненості інформаційного простору держави.

Погодимося із точкою зору, що існуючі у суспільстві соціальні норми, прагнення, потреби і громадська думка значною мірою формуються ЗМІ. Телебачення, радіо, Інтернет тощо, вступивши у комунікативні зв'язки із споживачами своєї продукції, зблизили усіх жителів одного "глобального селища" можливістю не тільки краще пізнавати одне одного, але й інформувати про одні Й ті ж теми приблизно в один і той самий час. Цей процес має одну характерну особливість: комунікація має односторонній характер, тобто

характер інформування. Ми маємо право довіряти або не довіряти отриманій інформації, але вступити у дискусію з телевізором чи газетою не можемо з тієї ж причини, з якої не говоримо з тролейбусом. Колонка "листи читачів" не виправляє зазначеного недоліку, оскільки у дискусію вступає лише мізерна частина споживачів інформації, а недоцільність публікування усіх листів надає можливість редакторам вибирати із маси листів лише ті, які відповідають поглядам ЗМІ.

Усі споживачі інформації через ЗМІ індивідуально обробляють однакові факти. Однак специфікою сучасних ЗМІ (а особливо найбільш поширених та ефективних з них - телебачення та радіомовлення) є те, що інформаційні повідомлення передаються не у вигляді власне фактів, а як готові твердження, висновки, аналітичні матеріали. Споживач позбавлений можливості вести дискусію з "опонентом" і найчастіше сприймає на віру якісно підготовлений матеріал від авторитетних джерел. Обговорення не є публічним у комунікаційному (не юридичному) розумінні - споживачі отримують інформацію особисто.

Тому це односторонній діалог: ЗМІ переконують. Як хрестоматійний приклад можна навести ситуацію, коли у 30-х роках XX ст. у Лондоні та Нью-Йорку вперше пустили в ефір радіопостановку "Війни світів" Герберта Уелса. Серед населення цих міст почалася паніка, спричинена уявним нашестям марсіан.

Мельниченко Георгій
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Кібербезпека – це сукупність умов, при яких всі складові кіберпростору захищені від максимально можливого числа загроз і впливів з небажаними наслідками. Інакше кажучи, це стан захищеності кіберпростору.

Інформаційні технології зараз стрімко розвиваються, створюючи серйозну проблему, а іноді загрозу для національної та міжнародної безпеки в усьому світі. В усіх країнах стрімко почалася розробка сучасної стратегії кібероборони. 15 березня 2016 року постанова Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» була введена в дію Указом Президента України. Також слід зазначити, що в Україні вже давно назріла необхідність в прийнятті положень щодо законодавства кібербезпеки, так як кіберпростір стає більш окремою, поряд з традиційними сферами («Земля», «Повітря», «Море», «Космос»), військова сфера, в яких відповідні спецпідрозділи збройних сил провідних держав стали діяти активніше. Беручи

за увагу широке використання сучасних інформаційних технологій у сфері оборони і безпеки, захист Україні з кожним днем стає все більш вразливим. Сучасний рівень кібербезпеки України є досить низьким, випадки незаконного збирання, зберігання, використання, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства стають все більш і більш поширеним явищем в Інтернеті. Мета нової стратегії кібербезпеки в Україні полягає в створенні умов для безпечної експлуатації кіберпростору, його використання в інтересах особистості, суспільства і держави.

Стратегія визначає, зокрема, такі основні пріоритети для безпечного, стабільного і надійного кіберпростору в Україні:

- Розробка та оперативна адаптація державної політики в сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС і НАТО;
- Створення національної нормативно-правової та термінологічної основи в цій сфері, гармонізація нормативних актів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів та стандартів ЄС і НАТО;
- Розробка технологій кібербезпеки мобільних засобів зв'язку;
- Розвиток електронної інфраструктури зв'язку;
- Розвиток і вдосконалення системи державного контролю інформаційної безпеки, а також незалежний аудит системи інформаційної безпеки;
- Розробка команд мережі реагування на комп'ютерні надзвичайні ситуації;
- Розвиток міжнародного співробітництва в сфері кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, активізація співробітництва між Україною та ЄС і НАТО з метою зміцнення можливостей України в сфері кібербезпеки.

У зв'язку з цим Стратегія визначає, що кіберзахист критичної інфраструктури повинен, зокрема, в першу чергу включати:

- Вдосконалення складної нормативно-правової бази кіберзахисту критичної інфраструктури;
- Організацію та ведення державного реєстру найважливіших об'єктів інфраструктури;
- Розробку і впровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами щодо загроз об'єктам критичної інформаційної інфраструктури.

Стратегія визначає мету створення **«активного кіберзахисту»**, що означає здійснення воєнно-політичних, воєнно-технічних та інших заходів, спрямованих на розширення прав і можливостей військової організації держави, сектора безпеки і оборони в кіберпросторі, створення, розвиток сил, засобів та інструментів для можливої відповіді на агресію у віртуальному просторі, що може бути використаний як засіб стримування воєнних конфліктів і загроз в кіберпросторі. Іншими словами, Україна створить механізм кібератак у відповідь.

Стратегія остаточно законодавчо визначає концепцію критичних об'єктів інфраструктури, таких як енергетичні і транспортні магістральні мережі, лінії нафто- і газопроводів, морські порти і т.д.

Надаючи спецслужбам інструменти он-лайн доступу до комп'ютерних даних абонентів, також важливо зберегти баланс між правом громадян на недоторканність приватного життя і інтересами національної безпеки.

Література:

1. "Питання створення "Огляду сектору кібербезпеки України""

2. ИСО/МЭК 27032:2012 Настанови щодо кібербезпеки «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо кібербезпеки » (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

3. УДК 323:351 Стратегічні аспекти кібербезпеки в Україні

Маслова Юлія
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОСНОВНІ ЗАГРОЗИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Загрози інформаційній безпеці — сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на такі групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації;
- загрози праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.

Фактори загроз за видовою ознакою поділяються на:

- політичні;
- економічні;
- організаційно-технічні.

Під політичними факторами загроз інформаційній безпеці розуміють:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;
- порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
- прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін.
- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;
- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері

Глобальні фактори загроз інформаційній безпеці:
- недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;
- діяльність іноземних розвідувальних та спеціальних служб;
- діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;
- злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:
- використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;
- невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;
- відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;
- недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;
- розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;
- зростання злочинності в інформаційній сфері;
- використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;
- відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:
- перехоплення електронних випромінювань;
- застосування підслуховуючих пристроїв або закладок;
- дистанційне фотографування;
- розкрадання носіїв інформації та промислових відходів;

- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне приєднання до апаратури та ліній зв'язку;
- упровадження та використання комп'ютерних вірусів і т. ін.

Література
1. «Стратегія забезпечення кібернетичної безпеки України» (від 15.03.2016 № 96/2016)
2. «Стратегія національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007)
3. Бурячок, В. Л. ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: СОЦІОТЕХНІЧНИЙ АСПЕКТ/ В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – Київ: ДУТ, 2015. – 287 с.

Хоменко Тетяна
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

НАЙБІЛЬШ ПЕРСПЕКТИВНІ ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

У числі технологій, які найближчим часом будуть чинити вирішальний вплив на розвиток телекомунікацій, слід назвати:
- Оптичні технології SDH / SONET, що забезпечують збільшення швидкості, здешевлення доступу до мережі, а отже, збільшення числа користувачів;
- Широкосмугові канали B-ISDN, що дозволяють передавати різнорідну інформацію з одного і того ж каналу і, як наслідок, підвищують швидкодію та інтелектуальність мережі;
- Єдину технологію мультиплексування і комутації ATM, що підвищує інтелектуальності мережі;
- Методи кодування і стиснення інформації, яким належить зіграти ключову роль в еволюції широкосмугових мереж, різко збільшивши передані інформаційні потоки і тим самим забезпечивши можливість передачі з високою якістю мультимедійної, телевізійної та іншої інформації (найбільш значущі стандарти стиснення: рекомендації МККТТ серії Н, стандарти JPEG і група стандартів MPEG-1, 2, 3, 4);
- Комутовані ЛВС (Fast Ethernet, FDDl FDDI II, ATM), збільшують продуктивність та інтелектуальність мережі;
- Цифрову бездротовий зв'язок, що сприяє зростанню числа і мобільності користувачів;
- Інтероперабельність мереж (Java)
- Універсальний доступ до послуг Internet (WWW).

Етапи розвитку телекомунікаційних технологій

У числі основних етапів розвитку телекомунікаційних технологій слід назвати:

- Телеграфні та телефонні мережі (докомп'ютерну епоху);
- Передача даних між окремими абонентами по виділених і комутованих каналах з використанням модемів;
- Мережі передачі даних з комутацією пакетів: дейтаграмному або використовують віртуальні з'єднання (типу X.25);
- Локальні обчислювальні мережі (найбільш поширені - Ethernet, Token Ring);
- Цифрові мережі інтегрального обслуговування (ISDN) - вузькосмугові, а потім широкосмугові;
- Високошвидкісні локальні мережі - Fast Ethernet, FDDI, FDDI II (розвиток FDDI для синхронної передачі мовної та відеоінформації);
- Високошвидкісні розподілені мережі Frame Relay, SMDS, ATM;
- Інформаційні супермагістралі.

Області застосування:

- Канали низького, середнього і високого якості;
- Широкий діапазон швидкостей передачі даних (від 1,2 Кбіт/с до десятків Мбіт / с.)
- Можливість використання як в розподілених, так і в локальних мережах.

За даними газети Financial Times, сьогодні в мережі Internet працює приблизно 40 мільйонів користувачів, об'єднаних більш ніж в 40 тис. Мереж. Кожні 30 хвилин до неї приєднується нова мережа і кожен місяць додається 1 млн. Нових користувачів. До 2000 року, як видно, число користувачів Internet перевищить 100 млн. Чоловік. Мережа Internet виникла в результаті проекту DARPA (Defence Advanced Research Projects Agency), який був початий в середині 70-х років і очолювався агентством Міністерства оборони США. До реалізації проекту були залучені наукові та технологічні ресурси університетських, промислових і урядових лабораторій США. Співрозробником телекомунікаційної інфраструктури стали Національний науковий фонд, Міністерство енергетики, Міністерство оборони, Агентство охорони здоров'я та гуманітарних послуг та NASA. Створену в результаті інтерсеть називають Connected Internet, DARPA / NFS Internet, TCP / IP Internet або просто Internet.

Сьогодні Internet являє собою транснаціональну інфраструктуру, яка об'єднує велику кількість різних комп'ютерних мереж, що працюють по найрізноманітніших протоколах, що зв'язують комп'ютери різних типів і забезпечують передачу даних в різних фізичних середовищах: телефонних кабелях, оптоволокне, радіо- і супутникових каналах.

Найбільш вражаючі успіхи телекомунікаційних технологій спостерігаються в останні 15 років.

Надалі основними напрямками еволюції телекомунікаційних технологій, мабуть, стануть:

- Збільшення швидкості передачі інформації, обумовлене зростаючими можливостями широкосмугових ліній і загальним використанням оптичних каналів;
- Інтелектуалізація мереж передачі інформації;
- Різке зростання числа і мобільності користувачів в зв'язку з здешевленням і мініатюризацією кінцевих засобів і застосуванням техніки бездротового зв'язку.

Література:
1.Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.
2. Телекомунікаційні мережі та їх інформаційні ресурси / / Москва, 1994.
3.Інтернет: енциклопедія / / Петербург, 2001.

Андрущенко Ярослав
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

“БЕЗОПАСНЫЕ” БЕСПРОВОДНЫЕ СЕТИ

В наше время огромное количество людей являются пользователями Интернета. Без него наша повседневная жизнь совсем невозможна.Мы сидим в нем часами напролет: читаем свежие новости, смотрим последние сводки спортивных мероприятий или же просто пытаемся убить время в ожидании, пока наша любимая девушка/супруга наконец-то соберется. Выходя на улицу, мы десятки раз обновляем наши социальные сети в ожидании сообщения от наших друзей. Когда интернета нет поблизости или же мобильный отказал, мы ищем место, куда бы нам “приконектится”, паникуя и бегая в поиске это желанной точки доступа. И вот, перед нами дверь с надписью “Free Wi-Fi”. Обычно, в этот момент люди испытывают что-то среднее между счастьем от продолжения нового сезона нашего любимого сериала и поездки “зайцем” в автобусе, когдаконтролер проходит мимо тебя. Мы находим укромное местечко в этом кафе и подключаемся к “всемирной паутине”. И вот мы начинаем “чатится” с нашими друзьями. Все проходит прекрасно, мы отсылаем забавные фото, пишем истории в «Twitter». Но никто не думает про то, что наша персональная информация может быть похищена. И то, что мы считали личным, сакральным попадает в руки нечестным людям. Эти люди используют весьма известные и распространенные способы атаки на пользователей. Одна из них – MITM (ManInTheMiddle). Этот тип атаки является очень успешным и совсем не сложным в реализации. Это нарушение закона, так как хищение персональных данных –наказуемо. И человек будет притянут к уголовной ответственности. Атака на жертву происходит за счет ARP- spoofing. Адресация

в сети выполняется за счет простого протокола ARP. Вкратце расскажу, что это. Это протокол физической адресации. Не важно, что у вас: компьютер, телефон, кофеварка или даже smart- холодильник. Все эти устройства имеют физический адрес. Так называемый MAC- адрес. Этот адрес указывается на сетевой карте. Число из шести битов. Пример MAC– адреса : 09-A3-0C-E9-D3-32. Первые три пары отвечают за фирму и модель устройства. А вторые три пары – это его уникальный номер. Любое устройство, которое имеет подключение к Интернету, имеет свой, уникальный номер. Вот мы немного и разобрались, что это такое. И как же этими знаниями можно воспользоваться? А все просто! MAC – адрес можно легко подменить. Меняя его, мы становимся тем, чей адрес мы возьмем. Мы можем стать кем угодно. Это как одевать маску и такую, что устройство не узнает вас настоящего. Но будьте осторожны, так как если вы возьмете случайный адрес, то можете стать принтером или той же кофеваркой. Забавно, не так ли?

И как же это все применить? Мы становимся промежуточным звеном между жертвой и роутером. Для жертвы мы роутер, а для роутера мы пользователь. Всю информацию мы пропускаем сквозь себя, тем самым мы получаемся все, что жертва смотрит в Интернете. Эта атака очень опасна, так как можно получить все. Мы можем при помощи определенных манипуляций получить даже логии и пароль от банковских карт, если пользователь решил проверить это в кафе. Получить доступ к почте, данные о соц. сетях. Но вы спросите, как это возможно, если есть такая крутая вещь, как SSL?Кто не знает, это криптографический протокол который используют HTTPS сайты. Он подразумевает более безопасную связь, так как использует асимметричную криптографию для аутентификации ключей обмена и симметричную для сохранения конфиденциальности.

И вот мы начинаем атаку. Есть два пути провидения атаки.

Первый : банальный перехват ваших “cookie”. После авторизации ваш диалог с сайтом основан на “кукисах”. Это файл, который находится навашем ПК и избавляет вас от необходимости постоянно вводить логин и пароль. Используя это, он может просто зайти под вашей учетной записью, но он не может получит логин и пароль.

Второй: более сложный и эффективный. Так как любому злоумышленнику нужен именно логин и пароль, для этого, нам нужно,что бы он ввел их повторно. Поэтому мы должны убить его “куки”. После этого ему придется ввести данные повторно и их можно перехватить. И вот мы завладели логином и паролем. Можем использовать, как хотим.

Так же, можно перехватывать SSL –трафик, потом его расшифровать и получить все,что там есть. Данные действия являются незаконными, как и все сказанное выше. Поэтому пробовать нужно только на своих сетях и устройствах.

Получив такие безмерные возможности, как посредничество между вами и роутером, он может изменить полностью всю информацию, которая приходит

к вам. Вплоть до того, что он может выбирать сигнатурно элементы для замены.

Подводя итог, хочу сказать: будьте бдительны и внимательны при использовании Интернета, ведь самая большая угроза для вашего компьютера – прослойка между компьютером и креслом. Берегите себя.

Седлецький Денис Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ІНТЕРНЕТ РЕЧЕЙ. ПЕРСПЕКТИВИ РОЗВИТКУ І БЕЗПЕКА

Кількість даних у Всесвітній мережі експоненціально зростає. Разом з тим зростають і загрози для користувачів і власників цих даних. Інтернет речей (Internet of Things або IoT) являє собою розумні пристрої, які роблять наше життя комфортнішим. Водночас із цим виникає питання безпеки. Інтернет речей є одним з найбільших джерел потенційних атак і головним болем для компаній, які працюють в сфері технологій керування даними.

Згідно з даними міжнародної консалтингової компанії IDC, очікується, що число IoT-пристроїв зростатиме з 15 мільярдів одиниць в 2016 році до 30 мільярдів в 2020 році. Великі підприємства мають в розробці широкий спектр таких проектів, але слабка взаємодія між цими корпораціями може призвести до великих проблем в безпеці таких пристроїв. За інформацією, представленою компанією HP у щорічному звіті дослідження «Enterprise Security Research» близько 80% цих пристроїв навіть не вимагають адекватного захисту паролем, 70% дозволяють хакеру отримати персональні дані користувача і 70% не шифрують дані, відправляючи їх в Інтернет або по локальній мережі. Для підприємств в сфері бізнес-технологій не може бути й мови про комфорт, припускаючи, що дані користувачів можуть бути викрадені. Все це свідчить про велику плутанину навколо Інтернету речей і безпеки.

Виявлення проблем

Пристрої IoT збирають, обробляють та аналізують величезні обсяги даних. Той факт, що більшість виробників мають слабке уявлення про те, скільки таких пристроїв в їх середовищі, свідчить про те, що питання безпеки все ще залишається відкритим. Основна проблема полягає в тому, що більшість таких девайсів виходять за межі традиційних методів забезпечення безпеки технологій, включаючи брандмауери та системи виявлення вторгнень. Проектування малопотужних процесорів для цих пристроїв значно обмежують технології і протоколи безпеки, які можуть бути застосовані до них. Інша причина – бюджетні обмеження. Підприємства давно зрозуміли, що вони не

можуть просто витрачати все більші і більші кошти на забезпечення безпеки, проте швидкість, з якою виникають нові загрози посилює тиск для збільшення інвестицій. Також варто враховувати дефіцит навичок із забезпечення безпеки інтернет речей. Прагнення виробників якнайшвидше випустити новий продукт задля здобуття конкурентної переваги, не залишає часу на опрацювання надійності та безпечності девайсу.

Шлях до безпеки IoT

Атака на пів терабіту – це вже серйозно, але в контексті розвитку інтернету речей це дрібниці. Розвиток IoT передбачає, що мережеві пристрої, що працюють автономно, будуть лічитись не сотнями тисяч, а десятками мільярдів. Якщо до цього часу не буде введено нові методи їх захисту і методи закриття вразливостей, у нас будуть проблеми. І, на відміну від теперішнього часу, коли ми можемо купувати інтернет-холодильник, а можемо і не купувати, вибору вже не буде. Вразливість, і, гірше того, неможливість оновлення програмного забезпечення мільярдів пристроїв призведе до маси проблем, які можуть торкнутися як нічого не підозрюють користувачів, так і вплинути на працездатність критично важливої інфраструктури. Які підходи можуть бути використані для захисту? Ринок рано чи пізно прийде до двох-трьох основних платформ, на яких будуть будуватися всі IoT-системи, і хаосу стане менше. Швидше за все так і буде, як це вже сталося з кількістю платформ для смартфонів в кінці нульових або операційних систем для ПК в 90-х роках минулого століття. А якщо ні? Концепція безпеки навряд чи повинна будуватися виходячи із законів ринку. До інтернету речей має бути інше ставлення, ніж до персонального комп’ютера і смартфону: окремі, захищені канали зв'язку, власні надійні методи авторизації, і головне - використання технологій, які максимально знижують ймовірність виконання чужого коду. Можливо, рішення цього питання буде знаходитися в поєднанні найсучасніших технологій. Програмуватися правильний IoT може зовсім не так, як це відбувається зараз з традиційними комп'ютерами. Можливо треба шукати інший підхід, не намагаючись затягнути в 21-е століття техногенну спадщину двадцятого століття.

Джерела:
IT-ресурс «Computerworld UK». URL: http://computerworlduk.com/
IT-ресурс «Хабрахабр». URL: http://habrahabr.ru/
Інтернет-ресурс компанії «Hewlett-Packard» http://hp.com/

Ковтун Юлія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПЕРСОНАЛ КАК ГЛАВНАЯ УГРОЗА ИБ.

Угрозы – неотъемлемая часть существования любой системы. Полностью обезопасить себя от них невозможно. Именно поэтому, минимизация угроз и убытков из-за них – приоритетная цель как человека отдельно, так и организации/предприятия в целом. Для этого создаются сложные системы защиты, которые обеспечивают безопасность системы на разных уровнях. Но какой бы «идеальной» система защиты не была, существует угроза, действия которой невозможно предсказать – это человек.

Что же такое угроза, а если точнее «угроза информационной безопасности»? **Угроза информационной безопасности** – совокупность условий и факторов, создающих опасность нарушения информационной безопасности. **[1]** Существует множество угроз и все их можно разделить по определенным характеристикам:

- По природе возникновения (естественные, искусственные);
- По степени преднамеренности проявления (непреднамеренные, преднамеренные);
- По непосредственному источнику угроз (природная среда, человек, программно-аппаратные средства);
- По положению источника угроз и т.д. (внешние, внутренние). **[2]**

Еще з давних времён, когда человечество начало задумываться про безопасность не только своей жизни, но и всего, что его окружало, самой главной угрозой оставался сам человек. Даже стремительно развитие технологий, методов и средств защиты, не может полностью обеспечить защиту от человеческого фактора.

Точно такую же тенденцию можно наблюдать и в ИБ. Используя самые новые технологии по защите информации, руководитель не может полностью уберечь ее от персонала, который имеет дело с ней.

Начиная от простой ошибки в запросе и заканчивая умышленным вмешательством в работу систем защиты – человеческий фактор непредсказуем. Существует множество факторов, способных влиять на действия человека. В основном, их делят на «позитивные» и «негативные» факторы, но, в априори, они равносильны друг другу. На каждый минус всегда найдется плюс. Каждый из них тем, или иным способом влияет не только на человека, но и на уровень угрозы, которую может представлять из себя личность.

Человек (персонал), исходя из вышеизложенного, относится к внутренним угрозам ИБ. И в этому случае, персонал может как непреднамеренно оказывать негативное влияние на ИБ (ошибки в процессе

работы с информацией и/или с системами защиты), так и преднамеренные (инсайдеры). Если инсайдера можно вычислить и ликвидировать (т.е. как-то обезопасить организацию от него), то уберечь предприятие от непреднамеренных угроз невозможно. Они, так или иначе, имеют место быть.

К непреднамеренным угрозам можно отнести:

- Уничтожение запрещенного для удаления файла;
- Изменение запрещенного для изменения файла;
- Некорректная установка программного обеспечения;
- Несоблюдение режима безопасности. **[3]**

Так же, в этот список мы можем отнести некоторые социальные состояния, такие как: паника, страх, всеобщая апатия и т.д. При каждом из этих состояний, персонал будет по-разному выполнять одну и ту же работу или задание. Любое действие в одном из названых состояний, либо любая названная угроза, могут привести организацию/предприятие к колоссальным убыткам. Контроль персонала под действием, например, паники, становиться практически невозможным.

Именно поэтому, руководителю следует, в первую очередь, быть как можно более внимательным к персоналу, который имеется в его организации. Если руководитель сможет правильно управлять подчиненными, шанс появления внутренних угроз, со стороны персонала, будет сводиться к минимуму. Традиционными методами управления персоналом можно назвать:

-Административные;

-Социально-психологические;

-Экономические. **[4]**

Пропорцию, какой метод и в каком соотношении с другими следует использовать, составляет сам руководитель. Именно от его действий и решений зависит уровень угроз со стороны человеческого фактора. Полностью, к сожалению, избавиться от такого типа угроз невозможно.

И в заключение, хотелось бы напомнить, что человек, сам по себе, непредсказуем. Именно поэтому, человеческий фактор стоит в самом верху потенциальных угроз ИБ.

Литература:

1. *Угрозы информационной безопасности. [Электронный ресурс]: (свободная энциклопедия) - Режим доступа - https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности*
2. *Анализ угроз информационной безопасности. [Электронный ресурс]: Режим доступа - http://ypn.ru/106/analysis-of-threats-to-information-security/*
3. *Виды и источники угроз информационной безопасности. [Электронный ресурс] – Режим доступа - https://sites.google.com/site/kontrolnaarabotapooek000123/teoriticeskij-vopros-no2*
4. *Методы управления персоналом. [Электронный ресурс] – Режим доступа - http://www.hr-director.ru/article/63435-red-qqq-15-m4-metody-i-printsipy-upravleniya-personalom-predpriyatiya*

Протасенко Костянтин Костянтинович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОРГАНІЗАЦІЙНО-РОЗПОРЯДЧЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розглянуто співвідношення служби захисті інформації в автоматизованих системах і служби інформаційної безпеки, запропоновано визначення служби інформаційної безпеки та окреслено основні організаційно-розпорядчі документи, що регламентують функціонування служби інформаційної безпеки підприємства, установи, організації.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1], що у свою чергу суттєво підвищує значення спеціалістів із захисту інформації.

Зазначені спеціалісти на підприємствах, в установах та організаціях входять до складу служби захисту інформації (далі – СЗІ), створення якої регламентовано Типовим положенням про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000), в якому також визначаються завдання, функції, структура, повноваження СЗІ, а також організації її робіт із захисту інформації впродовж всього життєвого циклу автоматизованих систем (далі – АС).

Зважаючи на те, що *захист інформації* – це діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому [2], а *інформаційна безпека* – це захищеність інформації та інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримуючої інфраструктури [3], можна встановити, що інформаційна безпека є більш ширшим поняттям ніж захист інформації

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від

форми, у якій вони перебувають. З метою забезпечення інформаційної безпеки на підприємствах, в установах, організаціях доцільно створювати службу інформаційної безпеки (далі – СІБ), яка складатиметься із спеціалістів СЗІ та спеціалістів інформаційної безпеки.

Нормативно закріплене визначення поняття «служба інформаційної безпеки» в Україні відсутнє, тому можна запропонувати таке визначення:

служба інформаційної безпеки – це організаційно-технічна одиниця системи забезпечення інформаційної безпеки, яка реалізує певні задачі, спрямовані на протидію загрозам інформаційній безпеці.

Підставою для створення СІБ є наказ (розпорядження) керівника підприємства, установи, організації, яким затверджується:

1) положення про СІБ;
2) склад СІБ;
3) інструкції співробітників СІБ.

Контроль за виконанням такого наказу (розпорядження) доцільно покласти на керівника підприємства, установи, організації.

Положення про СІБ є нормативним документом підприємства, установи, організації, що регламентує роботу служби, в якому визначаються завдання, функції, структура СІБ, повноваження та відповідальність співробітників СІБ, її взаємодія з іншими підрозділами підприємства, установи, організації та зовнішніми організаціями.

Положення про СІБ може бути складено у вигляді:

- доповнення до Положення про службу захисту інформації в автоматизованих системах – на підприємствах, в установах, організаціях, де наказом керівника затверджено положення про службу захисту інформації, створеної відповідно до НД ТЗІ 1.4-001-2000. У такому разі, в доповненні доцільно викласти:
  - завдання і функції спеціалістів СІБ, які не зазначені у положенні про службу захисту інформації;
  - структуру СІБ, розширену у порівнянні зі СЗІ;
  - взаємодію СІБ з іншими підрозділами підприємства, установи, організації та зовнішніми організаціями;
- окремого документа, складеного на базі положення про СЗІ – на підприємствах, в установах, організаціях, де не було створено СЗІ та прийнято рішення про створення СІБ.

З метою забезпечення кібербезпеки, організації та здійснення ефективної боротьби із кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю, забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, до складу СІБ доцільно включити спеціалістів із кіберзахисту. Завдання та функції таких спеціалістів викладені у розділі 4 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016.

Особи відповідальні за зберігання матеріальних носіїв інформації здійснюють свою діяльність відповідно до вимог Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 № 939, Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженої постановою Кабінету Міністрів України від 19.10.2016 № 736, та інших нормативно-правових актів.

У залежності від обсягів і особливостей завдань СІБ до її складу можуть входити спеціалісти різного фаху:

- спеціалісти з питань захисту інформації від витоку технічними каналами;
- спеціалісти з питань захисту каналів зв'язку і комутаційного обладнання, налагодження і керування активним мережевим обладнанням;
- спеціалісти з питань адміністрування засобів захисту, керування базами даних захисту;
- спеціалісти з питань захищених технологій обробки інформації»
- спеціалісти з кіберзахисту;
- особи відповідальні за зберігання матеріальних носіїв інформації;
- спеціалісти, відповідальні за встановлення та експлуатацію інженерно-технічних засобів охорони та інші.

За посадами співробітники СІБ поділяються на такі категорії (за рівнем ієрархії):

- керівник СІБ;
- заступник керівника СІБ (у разі необхідності);
- адміністратори захисту АРМ (безпеки БД, безпеки систем, документів тощо);
- системні адміністратори;
- інженери з кіберзахисту;
- інженери з експлуатації інженерно-технічних засобів охорони;
- фахівці із захисту матеріальних носіїв інформації;
- інші спеціалісти СІБ.

СІБ може бути штатним підрозділом підприємства, установи, організації, безпосередньо підпорядкованим керівнику, який відповідає за забезпечення безпеки інформації, або структурною (штатною або позаштатною) одиницею підрозділу служби безпеки підприємства, установи, організації, в разі їх наявності.

Штатність чи позаштатність СІБ на підприємстві, установі, організації визначається рішенням керівництва підприємства, установи, організації відповідно.

Структура СІБ, її склад і чисельність визначається фактичними потребами підприємства, установи, організації для виконання вимог політики безпеки інформації та затверджується керівництвом. Чисельність і склад СІБ мають бути достатніми для виконання усіх завдань з інформаційної безпеки підприємства, установи, організації.

Інструкції спеціалістам СІБ складаються за прийнятою на підприємствах, установах, організаціях формою та, як правило, містять:

- загальні положення;
- обов'язки спеціаліста;
- права спеціаліста;
- відповідальність спеціаліста.

СІБ здійснює свою діяльність щодо реалізації основних організаційних та організаційно-технічних заходів зі створення і забезпечення функціонування комплексних систем захисту інформації та комплексів технічного захисту інформації у відповідності з планами робіт. Підставою для розроблення планів робіт є:

- план захисту інформації в АС, що є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу АС;
- план технічного захисту інформації (далі – ТЗІ) підприємства, установи, організації, що повинен містити такі документи:
  - перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;
  - інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;
  - інструкції, що встановлюють обов`язки, права та відповідальність персоналу;
  - календарний план ТЗІ.

Календарний план може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи.
- робота з кадрами.

До планів включаться наступні основні заходи:

- разові (одноразово виконувані, необхідність у повторенні яких виникає за умови повного перегляду прийнятих рішень з захисту інформації);
- постійно виконувані (заходи, що потребують виконання безперервно або дискретно у випадковий чи заданий час);
- періодично виконувані (з заданим інтервалом часу);
- виконувані за необхідності (заходи, що потребують виконання під час здійснення або виникнення певних змін в АС чи зовнішньому середовищі).

За результатами виконання планів СІБ готуються звіти про забезпечення безпеки інформації на підприємствах, в установах, організаціях, які регулярно (наприклад – щоквартально) подаються керівництву.

У звітах відображається стан інформаційної безпеки на підприємствах, в установах, організаціях, із зазначенням досягнутих показників і виявлених недоліків, робиться висновок і надаються пропозиції щодо покращення стану інформаційної безпеки.

Матеріально-технічну базу для забезпечення діяльності СІБ складають засоби захисту інформації, програмне забезпечення, технічне та інженерне обладнання, засоби вимірювань і контролю, відповідна документація, а також інші засоби та обладнання, які необхідні для виконання СІБ покладених на неї завдань.

СІБ фінансується за рахунок:

- коштів, що виділяються на підприємствах, в установах та організаціях на утримання органів управління;
- прибутку підприємств і організацій та інших коштів за рішенням керівництва;
- коштів, отриманих за виконання СІБ договірних робіт та надання послуг;
- інших джерел фінансування, не заборонених законодавством України.

На підставі викладеного вище, зважаючи на необхідність захисту інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, незалежно від форми, у якій вони перебувають, у подальших дослідженнях за темою статті доцільно розглянути нормативно-правові та інші питання щодо створення, організації та забезпечення функціонування служби інформаційної безпеки підприємства, установи, організації.

Література:

1. Стратегія кібербезпеки України затверджена Указом Президента України від 15 березня 2016 року № 96/2016[Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/96/2016
2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343
3. Берко А.Ю., Висоцька В.А., Рішняк І.В. МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОЇ [Електронний ресурс] / Берко А.Ю., Висоцька В.А., Рішняк І.В. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/natural/Vnulp/Komp-systemy/2007_591/14.pdf

Афонин Е.С.
Государственный университет телекоммуникаций
Учебно-научный институт Телекоммуникаций и информатизации
Факультет телекоммуникаций
г. Киев

Гуменная А.А
Национальный авиационный университет
Институт аэроавиации
Факультет телекоммуникаций
г. Киев

ПРИЕМНИК ДЛЯ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ КОММУНИКАЦИИ С ВЫСОКОЙ ФОТОЧУВСТВИТЕЛЬНОСТЬЮ

В статье изложены результаты изучения фото детектирования при барьерной модуляции в $Au - CdP_2$ структурах. Предоставлены результаты исследования спектральных и частотных характеристик фотодиода с баоьером Шоттки. Показана перспективность использования прибора для оптико-волоконных систем коммуникаций. Предложена физическая эвивалентная схема фотодиода. Рассмотрена комбинация фотодиода и элекктрического усилителя (макет приемного оптического модуля).

Для приема информации в системах системах оптической связи (ОС). (в условиях малых световых потоков) необходимо значительное повышение чувствительности фотодетекторов. Для этого важно, как использование новых фоточувствительных материалов, так и модернизация приборов, изготавливаемых на их основе.

В настоящей работе предлагается использование кристаллов CdP_2 ит разработка на их основе фотодиода Шоттки. Наличие инварианта Лифшица, который описывает эти кристалы со структурой D_4^4 , обусловливает флуктационный фазовый переход и возникновение естественной сверхрещетки (СР). Всвою очередь наличие СР резко повышает фоточувствительность (ФЧ) этих кристалов.

Далее существенное увеличение ФЧ можно реализовать за счет использования фотодиода Шоттки при создании определенного профиля легирования полупроводниковой подложки.

Структура фотодиода и его характеристики.

Была изготовлена структура $Au - CdP_2$ с поверхностным компенсированным слоем. Кристаллы обладали дырочной проводимостью($p - CdP_2$) . Компенсированый слой получали с помощью

имплантаци на глубину 0,1…0,2 мкм. Концентрация компенсированой примеси (Nd) превышала концентрацию акцепторной примеси (Na):
Nd> Na ~2×10^{10}см$^{-3}$
Результирующее распределение потенцияала и объемного заряда приведено на рисунке 1:

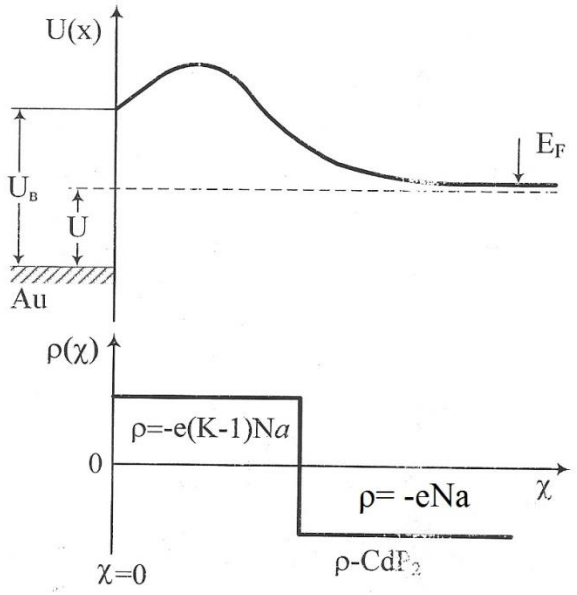


Рисунок 1. Распределение потенциала и объемного заряда в системе $Au - CdP_2$

Высота U_h образующегося потенциального «горба» может быть определена с помошью следующего выражения:

$$U_h = \frac{\varphi_{ii} - Å_F}{K_n - 1}\frac{d^2}{l^2}\left[K_n - \left(\frac{l^2}{d^2} + K_n\right)^{\frac{1}{2}}\right]^2$$

где $\varphi_{мп}$- высота барьера Шоттки;
E_F- энергия Ферми;
l- глубина слоя истощения;
d- глубина компенсированного слоя;
K_n- результат соотношения N_d/N_a.

При освещении высота U_h уменьшается, что приводит к уменьшению величины K_n. В результате при приложении к структуре смещения в прямом направлении происходит усиление фототока в 10^6 раз.

Пороговая чувствительность составляла 5×10^{11} фотон/см$^{-2}$. Время релаксации 10^3с. Добротность фотоприемника достигала 2×10^8 с$^{-1}$, что являтся весьма высоким значением.

Литература:
Андреева Н.О., Дружинин В.А., Зуев В.А. ПРИЕМНИК ДЛЯ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ КОММУНИКАЦИИ С ВЫСОКОЙ ФОТОЧУВСТВИТЕЛЬНОСТЬЮ

Курбанов Джахангір Абдуллайович
Держаний університет телекомунікацій
Навчально-науковий інститут
менеджменту та підприємництва
Туркменістан

СТРАТЕГІЇ УПРАВЛІННЯ ІННОВАЦІЙНИМ РОЗВИТКОМ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ

Розглянуто види та принципи формування стратегій управління інноваційним розвитком сучасних телекомунікаційних підприємств. Наголошено, що інноваційним розвитком вважається розвиток, який спирається на безперервний пошук і використання нових способів і сфер реалізації потенціалу телекомунікаційного підприємства, окреслено основні особливості розробки стратегій управління інноваційним розвитком сучасних телекомунікаційних підприємств, врахування яких дозволить сформувати моделі їхнього інноваційного розвитку, ефективно управляти інноваційними процесами.

Процеси глобалізації і зміни у співвідношенні факторів економічного зростання, унаслідок яких на перше місце вийшли інновації і інноваційна діяльність з опорою на інформацію і знання, сьогодні активізували пошук шляхів забезпечення конкурентоспроможності національних економік та окремих підприємств. Нині, здатність до створення, використання й збільшення інтелектуального капіталу визначають економічну могутність держави, добробут і якість життя народу. У сучасному світі активно відбувається перехід від конкуренції на основі фінансового капіталу, факторів виробництва та інвестицій до конкуренції на основі нововведень.

З позиції конкретних телекомунікаційних підприємств інноваційну діяльність необхідно розглядати як один з основних засобів їх адаптації до постійних змін умов зовнішнього середовища. Інноваційним вважається розвиток, який спирається на безперервний пошук і використання нових способів і сфер реалізації потенціалу телекомунікаційного підприємства в мінливих умовах зовнішнього середовища в межах обраної місії та прийнятої мотивації діяльності і який пов‘язаний з модифікацією наявних і формуванням нових ринків збуту.

Л. Водачек і О. Водачкова розрізняють чотири основних типи інноваційної стратегії: активно наступальну, помірно наступальну, захисну і залишкову [1]. За класифікацією Х. Фрімана існує шість типів інноваційної стратегії підприємства: наступальна, захисна, імітаційна, залежна, традиційна та «за нагодою» [2]. К. П. 190 Янковський та І. Ф. Мухарь до наступальних відносять агресивні та помірковані інноваційні стратегії, а залишкову та адаптивну відносить до стратегій оборонного типу [4]. У загальному випадку розрізняють два типи ринкових стратегій функціонування телекомунікаційного підприємства: стабілізаційні – збереження досягнутого рівня виробництва, частки ринку тощо; розвивальні – розширення виробництва, частки ринку, збільшення прибутку тощо.

Однак, як свідчить практика, перші можуть мати тільки тимчасовий успіх, але не здатні забезпечити тривалого виживання телекомунікаційних підприємств на ринку відповідно до їх місії і прийнятої мотивації бізнесу.

Процес інноваційного розвитку необхідно, насамперед, розглядати з позицій конкретного телекомунікаційного підприємства, що здійснює інноваційно орієнтовану діяльність у взаємодії з партнерами, конкурентами, торговими і збутовими посередниками, споживачами тощо у конкретних економічних, політичних, екологічних, правових та інших умовах. При цьому така взаємодія має ймовірнісний характер і не може бути оцінена однозначно.

Телекомунікаційне підприємство, що обрало інноваційний шлях розвитку, повинне функціонувати згідно з принципами: адаптивності, динамічності, самоорганізації, саморегуляції, саморозвитку. За цими принципами має функціонувати і система управління інноваційним розвитком телекомунікаційних підприємств. Управління інноваційним розвитком орієнтоване на досягнення поставлених цілей (захоплення більшої частки ринку, збільшення прибутку в поточному періоді чи в перспективі, забезпечення високих темпів стійкого економічного розвитку і т.п.) в умовах конкурентного середовища. Ці цілі слід належним чином узгоджувати з можливостями їх досягнення.

Серед головних особливостей розроблення інноваційної стратегії розвитку телекомунікаційних підприємств слід виділити [3]: специфіку методів ринкових досліджень, що передують розробленню нововведень (новацій); збільшення глибини прогнозування майбутнього розвитку подій як результату інноваційної діяльності; різке збільшення обсягів інформації, що переробляється, безупинне її накопичення й аналіз з метою обґрунтованого ухвалення управлінських рішень, своєчасного реагування на можливості і загрози, що з'являються на ринку; багатоваріантний характер прогнозів,

оскільки, як правило, розвиток подій може проходити декількома можливими напрямками, імовірності яких різні; оцінку здатності підприємства сприймати інновації (аналіз інноваційного потенціалу); детальний аналіз чинників ризику й оцінка ступеня їхнього впливу; ретельний добір методів і джерел фінансування інновацій, враховуючи детальний аналіз альтернативних варіантів; тісне ув'язування цілей, етапів і термінів реалізації стратегії з прогнозованими параметрами стадій життєвого циклу нововведення; високі мобільність і адаптивність стратегії, можливість її оперативної переорієнтації стосовно до змін умов зовнішнього і внутрішнього середовища господарювання; необхідність оцінки інноваційної стратегії за комплексом різних критеріїв (багатокритеріальна оцінка стратегії).

Кожне телекомунікаційне підприємство враховує різні особливості, що підвищує точність оцінки, знижує ймовірність упустити що-небудь. Урахування відзначених особливостей дозволить підвищити ефективність розроблення інноваційних стратегій 191 розвитку телекомунікаційних підприємств, сформувати моделі їхнього інноваційного розвитку, ефективно управляти інноваційними процесами.

Література:

1. Водачек Л. Стратегия управления инновациями на предприятии : [сокращ. пер. со словац.] / Л. Водачек, О. Водачкова. – М. : Экономика, 1989. – 166 с.
2. Інноваційний розвиток промисловості України / О. І. Волков, М. П. Денисенко, А. П. Герчан та ін. ; під ред. О. І. Волкова, М. П. Денисенко. – К.: КНТ, 2006. – 648 с.
3. Ілляшенко С.М. Управління інноваційним розвитком: Навчальний посібник. – 2-ге вид., перероб. і доп. – Суми: ВТД ‖Університетська книга‖; К.: Видавничий дім «Княгиня Ольга», 2005. – 324 с.
4. Янковский К.П. Организация инвестиционной и инновационной деятельности. / К. П. Янковский, И. Ф. Мухарь. – СПб.: Питер, 2010. – 448 с.

Хобта Б.М., Хобта П.М.

Государственный Университет Телекоммуникаций

Научно-исследовательский институт Телекоммуникаций и информатизации

Факультет Информационных технологий

г. Киев

FIREBASE И ОБЛАЧНОЕ ТЕСТИРОВАНИЕ ANDROID ПРИЛОЖЕНИЙ

Исследуются облачные сервисы Google Firebase и особенности тестирования работы мобильных приложений в Firebase Test Lab. Приведены основные факторы привлекательности пользовательского интерфейса. Рассматриваются пригодные для компаний способы борьбы с ошибками в программном обеспечении и их преимущества. Акцентируется внимание на Google Firebase как многоперспективном сервисе предоставления облачных технологий и как технологии предоставления NOSQL БД для real-time приложений.

На сегодняшний день, существует огромное разнообразие мобильных устройств. При этом, основным требованием к программным продуктам является надежность системы информационного обмена, простота и привлекательность пользовательского интерфейса [1, с. 92-94]. Надежность реализуется оконечным шифрованием, а привлекательность – понятие субъективное и зависит от многих факторов, основные приведены на рисунке 1.

Рисунок 1 Основные факторы привлекательности

Разработчику мобильных приложений важно знать мнение о своем продукте, но узнать его путем прямого опроса очень затруднительно и проблематично. Это критически важно для приложений, проходящих альфа-тестирование. На этом этапе разработчиками совершается огромное количество правок и ошибок [1, с. 210]. Наиболее критичными являются ошибки, что появляются во время выполнения приложения. Для компании разработчика программного обеспечения есть несколько выходов: 1) включить в штат сотрудников тестировщиков и обеспечить их необходимым аппаратным обеспечением; 2) создать социологический опрос пожеланий пользователей; 3) использовать готовые облачные средства сбора и анализа данных (Рис. 2) [2, с. 87;1, с. 102-103].

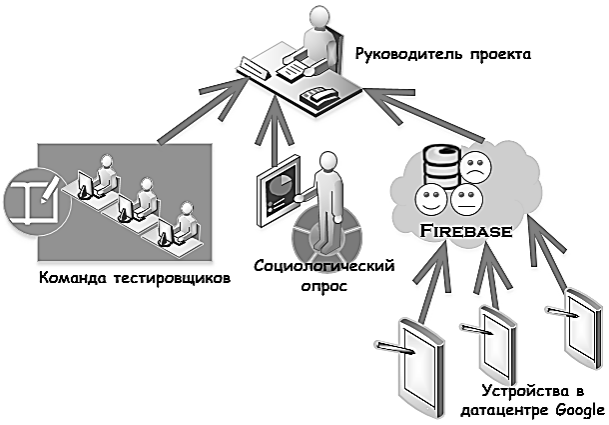


Рисунок 2 Способы анализа качества работы

Преимуществом первого способа есть точная гарантия качественной работы приложения на конечном числе устройств, а недостатком высокая стоимость закупаемой аппаратуры и увеличение штата сотрудников. Второй способ также требует расширения штата сотрудников и потребляет время пользователя. Он раздражает клиента и не гарантирует получения точной информации. Третий способ заключается в использовании Firebase test lab [2, с. 54].

Firebase это реализация облачной услуги BaaS (Backend as a Service) и заключается в том, что пользователю предоставляется готовое пространство для хранения баз данных и API интерфейс для удаленной работы с ними со стороны клиента (рис. 3) [3, с. 35].

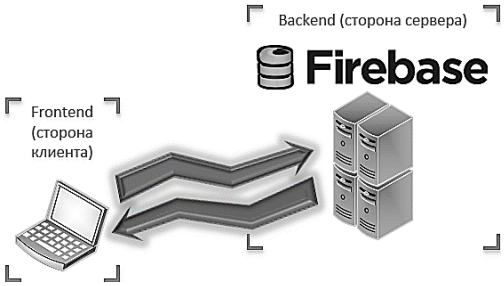


Рисунок 3 Общая схема работы услуги

После регистрации на сервисе Google Firebase и выбора тарифного плана, разработчик получает в свой арсенал возможность тестировать приложения на желаемых устройствах. Результаты всех тестов легко будут доступны из браузера разработчика. Firebase не похож на основные существующие базы данных. Все данные хранятся в форме JSON (javascript object notation) [4, с. 82]. Данные о тестировании на определенных устройствах хранятся в базе матриц результатов (рис. 4).

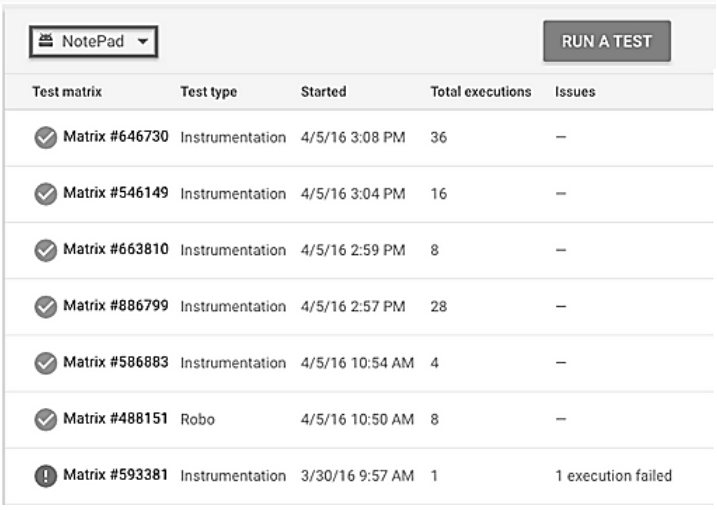


Рисунок 4 Матрицы результатов

После выбора тестовой матрицы браузер получит следующий JSON ответ:


```
{
 "matrix": "#658713",
 "type": "Robo test",
 "failed": 0,
 "passed": 2,
 "skipped": 0,
 "inconclusive": "ROBO",
 "date": {
 "day": 3,
 "month": 10,
 "year": 16,
 "hour": 1,
 "minute": 1,
 "daytime": "PM"
 }
 "dev_vendor": "Asus"
 "dev_name": "Nexus 7",
 "api_level": 21,
 "locale": "en_US",
 "duration": {
 "hours": 0,
 "minutes": 2,
 "seconds": 44
 }
 "orientation": "Landscape",
}
```


В браузере JSON ответ приобретет указанный на рисунке 5 вид.

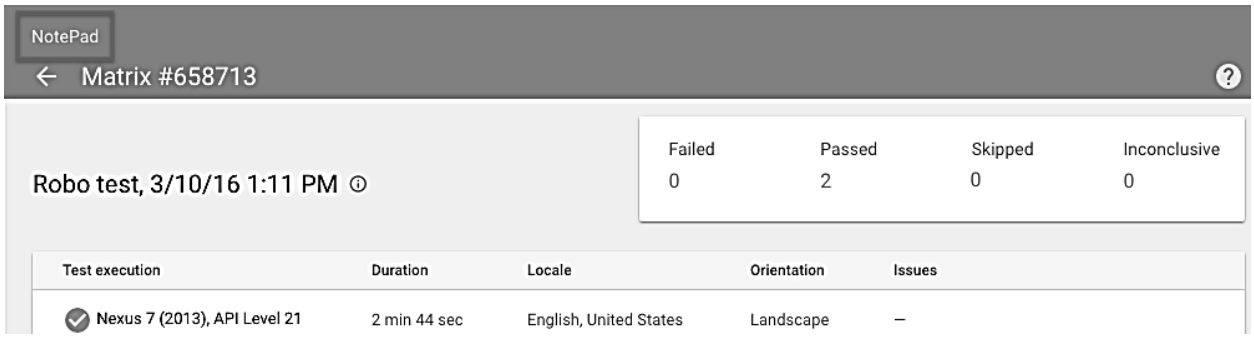


Рисунок 5 Просмотр матрицы тестирования

Выбрав элемент из колонки Test execution можно посмотреть результаты тестов, скриншоты приложения, и видео работы тестируемого приложения (рис. 6).

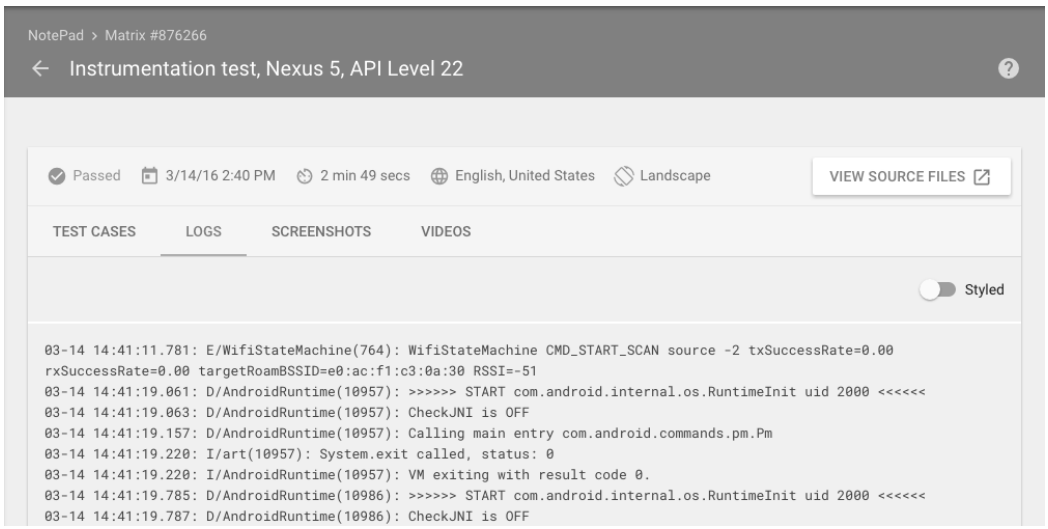


Рисунок 6 Подробный результат тестов

Использование Firebase test lab решает следующие задачи:

- избавляет от необходимости расширять штат сотрудников, производя роботизированный тест элементов приложения;
- избавляет от необходимости покупки аппаратуры для тестировщиков;
- выводит полный отчет (логи, скриншоты и видео) о работе приложения на целевом устройстве;
- позволяет избежать незаметных ошибок во время выполнения приложения;
- позволяет избежать раннего разочарования пользователей приложением.

Все перечисленные выше задачи являются ключевыми в процессе создания конечного востребованного рыночного продукта.

Литература

1. Алан Купер Об интерфейсе. Основы проектирования взаимодействия. – Пер. с англ. – СПб.: “Символ-Плюс”, 2009. – 688 с., ил.
2. Manoj Waikar Data-oriented Development with AngularJS. – Birmingham:”Packt Publishing Ltd”, 2015. – 156p.
3. *Donald Norman* The Design of Everyday Things. – New York:”BASIC BOOKS”, 2014. –369p.
4. Jenifer Tidwell Designing Interfaces. 2nd edition, Toronto:“O’Reilly Media”, 2010. –577p.

Говорун Олександра
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ЕЛЕКТРОННА КОМЕРЦІЯ: ПЕРЕВАГИ ТА НЕДОЛІКИ

Під поняттям електронної комерції розуміють будь-який вид ділової активності суб’єктів господарювання, що провадиться з використанням сучасних

інформаційних технологій, систем та комунікаційних засобів з метою отримання прибутку та задоволення потреб споживачів.

Електронна комерція як система включає в себе: суб'єкти електронного бізнесу (виробники, продавці, посередники, покупці, споживачі), процеси (реалізація продукції та послуг, маркетинг, розрахункові операції тощо) та мережі (як внутрішньофірмові, так і глобальні). Всі компоненти електронної комерції перебувають у взаємозв'язку завдяки засобам мережевого зв'язку. Оскільки для вітчизняного ринку електронна комерція є досить новим явищем, як для виробника, так і для споживача важливо оцінити з одного боку ті вигоди, які принесе участь у електронному бізнесі, а з іншого – потенційні проблеми, що можуть постати на шляху їх взаємодії. Вважаємо, що є необхідним систематизація як переваг, так і проблем впровадження електронної комерції в розрізі її суб'єктів, оскільки один й той самий пункт для виробника може бути перевагою, а для споживача – проблемою чи навпаки.

Таким чином, доцільно систематизувати переваги електронної комерції наступним чином:

1) для споживачів:

- нижчі ціни у порівнянні з традиційними магазинами (за рахунок зменшення невиробничих витрат підприємства електронної комерції мають можливість оптимізувати цінову політику);
- доступність інформації про товари, послуги в Інтернет-магазинах у режимі реального часу цілодобово без вихідних.
- використання торгівельних платформ, інтернет-магазинів, сайтів-агрегаторів інтернет-магазинів з метою вивчення ринку товарів та послуг, порівняння їх характеристик, цін (зокрема відкритість інформації, цінової політики не дозволяє недобросовісним продавцям необґрунтовано завищувати націнки, оскільки споживач може швидко порівняти ціни та обрати більш вигідну пропозицію);
- можливість купувати елітні, рідкісні товари у зарубіжних магазинах, на аукціонах, резервувати місця в готелях різних країн та отримувати інші високоякісні послуги іноземних компаній;
- наявність пошукових систем, які дозволяють споживачам знайти інформацію про необхідні товари та послуги (послуги пошуку надають або безпосередньо виробники або ж спеціалізовані сайти, які агрегують інформацію із сайтів електронних магазинів);
- можливість конфіденційного здійснення покупок;
- зменшення ймовірності здійснення транзакції з несумлінними, недосвідченими продавцями;
- можливість отримати швидко, просто безкоштовні зразки та скористатись фірмовою доставкою товарів від виробника;

- цифрові продукти, нематеріальні товари можуть бути одразу доставлені до споживача через мережеві канали;
- можливість обміну відгуками про товари та послуги, а також їх пошуку через соціальні мережі, спільноти, блоги тощо.
- більша відкритість компаній до споживачів.

2) для виробників:

- зниження обсягу первісних вкладень в бізнес (зникає потреба в купівлі чи оренду великих торговельних площ, торговельного обладнання), невиробничих витрат (витрат на рекламу, витрат,пов'язаних з сервісним обслуговуванням та інформаційною підтримкою споживачів);
- зменшення чисельності персоналу та фонду оплати праці, що обумовлено повною або частковою автоматизацією процесів, спрощенням комунікації в межах підприємства;
- скорочення циклу виробництва та продажу, підтримка бізнес-процесів у режимі on-line;
- зручність проведення маркетингових досліджень (зокрема якісна сегментація клієнтів, використання CRM, Customer Relationship Management, Google Analitycs, Яндекс метрика та ін.);
- великий потенціал розвитку системи роботи із клієнтами, без ризику, що система «знайде» собі інше місце роботи, як це нерідко відбувається із продавцями, що набрали досвід;
- надання нових видів послуг та освоєння нових сегментів ринку, глобальний доступ до світових ринків;
- рівність умов доступу до ринку як для великих корпорацій, так і для невеликих підприємств;
- цілеспрямований адресний вплив на споживацький сегмент за допомогою індивідуальних електронних засобів зв'язку;
- можливість роботи в режимі цілодобового доступу та інтерактивного спілкування із споживачем;
- пільгові умови оподаткування та сплати митних платежів;
- підвищення рівня прихильності споживачів до торгової марки.

3) для ділових контрагентів:

- оперативність отримання інформації, в тому числі при міжнародних операціях;
- поліпшення бізнес-контактів (е-комерція – B2B), можливість співпраці із партнерами незалежно від географічних кордонів.

4) для держави та суспільства:

- широкий асортимент товарів та послуг, що надаються населенню у різних сферах;

- нарощування потужності національної економіки, надходження інвестицій, розвиток інфраструктури, науки та техніки, підвищення рівня життя населення, зменшення «цифрового» розриву;
- створення нових робочих місць;
- підвищення рівня національної безпеки;
- за рахунок здійснення покупок в мережі зменшується автомобільний трафік та відповідно забруднення навколишнього середовища.

З іншого ж боку, електронна комерція має і негативні аспекти, які були згруповані за таким же принципом як і вигоди:

1) для споживачів:

- через засоби ідентифікації особи користувача можна здійснювати контроль за нею, перевіряти її діяльність;
- сегмент населення, що не має доступу до мережі залишається неохопленим, до того ж не всі види товарів є представленими в мережі;
- споживачі не мають змоги в повній мірі пересвідчитись у якості товару чи послуги до моменту отримання його;
- необхідність сплати авансу в повному або частковому обсязі від вартості покупки;
- складний порядок повернення товарів у випадку бажання клієнта повернути покупку;
- логістика виконання замовлення має швидкість, або продуктивність, неадекватну швидкості Internet, окрім того зростає вартість невеликих замовлень за рахунок поштових послуг, послуг перерахунку коштів;
- хаос, заплутаність і громіздкість Internet;
- відсутність мотивів відвідування магазинів, безпосередньо не пов'язаних зі здійсненням купівель.

2) для виробників:

- у системі електронної торгівлі упускається ефект, можливий тільки при особистому контакті покупця й продавця і, що досягає за рахунок чарівності продавців, їхніх інтуїтивних здатностей й уміння продати навіть не занадто бажаний для покупця товар;
- посилення конкурентної боротьби, її перехід на глобальний рівень, до того ж для країн, що розвиваються є характерним низький рівень охоплення населення мережею;
- необхідність забезпечення потужної технологічної основи для функціонування е-комерції, її постійного оновлення вимагає значних вкладень фінансових ресурсів;
- проблеми ціноутворення, так як внаслідок відкритості інформації виробники не можуть завищувати ціни;

- складність організації діяльності та розробки онлайн-вітрини (висока вартість, необхідність координації роботи відділу продажів, бухгалтерії, автоматизація обробки платіжних банківських карт і електронних грошей);
- внаслідок відкритості інформації зростає ймовірність порушення прав інтелектуальної власності, плагіату, фінансових шахрайств, тому постає проблема інформаційної безпеки;
- невизначеність та складність організації бухгалтерського обліку, внутрішнього контролю, переорієнтація інформаційних потоків із традиційних паперових носіїв у електронну форму, що за умов необізнаності працівників може ускладнити прийняття управлінських рішень;
- недостатня обізнаність працівників із сучасними інформаційними технологіями та системами, а висококваліфіковані кадри зазвичай вимагають значних витрат на оплату праці;
- необхідність залучення спеціалістів, що будуть здійснювати адміністрування сайту, оновлювати контент інформаційного ресурсу.

3) для ділових контрагентів:

- за умов існування е-комерції посередництво втрачає свої позиції, а тому взагалі може зникнути;
- необхідність підвищеної довіри між партнерами, фінансових та інших гарантій, оскільки реальне існування контрагента є невизначеним;
- необізнаність контрагентів із правилами ведення іноземного бізнесу, відсутність уніфікованих стандартів взаємодії в мережі можуть призвести до виникнення непорозумінь та конфліктів;
- складність координації економічних відносин, що складаються на віртуальному ринку із матеріальними аспектами цих відносин.

4) для держави та суспільства:

- нерівномірність розвитку електронної комерції у різних регіонах, галузях та в різних ланках виробництва;
- для країн з невисоким економічним розвитком електронний бізнес не є пріоритетним напрямом розвитку, окрім того вимагає вкладень в розвиток науки, техніки, інфраструктури;
- монополізація ринків, оскільки сектор малого підприємництва не завжди може вистояти перед викликами конкурентного середовища;
- внаслідок ускладнення контролю товарно-грошових потоків в мережі, правову невизначеність, створюються сприятливі передумови, які часто використовуються недобросовісними платниками податків для здійснення протиправної діяльності, зокрема, ухилення від оподаткування чи незаконної мінімізації сплати податків, різного роду шахрайств та зловживань.

Таким чином, кожен із потенційних учасників електронної комерції оцінивши наведені переваги та недоліки, зможе оцінити доцільність власної

участі у електронному сегменті економіки. Переваги та недоліки електронної комерції були доповнені та систематизовані в розрізі суб'єктів електронного бізнесу: виробники, споживачі, ділові контрагенти, суспільство. Така систематизація є об'єктивно необхідною, оскільки одній й ті ж вигоди для одного суб'єкта, можуть бути проблемою для іншого. Такий підхід дозволити підвищити рівень обізнаності учасників електронної комерції. На мій погляд, вигоди від розвитку електронної комерції є значно суттєвішими, ніж її недоліки, а тому виробники, ділові контрагенти, споживачі та суспільство в цілому зможе перейти на вищий щабель розвитку завдяки сучасним технологіям, а потенційні ризики можна зменшити шляхом впровадження надійних засобів електронної безпеки транзакцій, врегулювання на державному рівні проблем нормативно-правового регулювання цієї сфери тощо. До того є суб'єктам підприємницької діяльності не обов'язково, а іноді і зовсім неможливо, переносити повністю свій бізнес у мережу, в таких випадках буде ефективним поєднати дві моделі організації бізнесу «он-лайн» та «оф-лайн».

Література:

1. Возний М. І. Міжнародна електронна торгівля. Проблеми та перспективи розвитку в Україні /М. І. Возний // Збірник наук. праць Буковинського університету. Економічні науки. — 2011. — Вип. 7. — С.243–252.
2. Одарченко А. М. Особливості електронної комерції та перспективи її розвитку в Україні/ А. М. Одарченко, К. В. Сподар// Бізнес Інформ. – 2015. – №1. – С. 342–346. // Бізнес Інформ. – 2015. – №1. – С. 342–346.
3. Філіппова Л. Л. Електронна комерція: за і проти / Л. Л. Філіппова // Вісник Нац. техн. ун-туХПІ. –Харків : НТУ "ХПІ". – 2013. – № 44 (1017). – С. 58-65.
4. Ховрак І. В. Електронна комерція в Україні: переваги та недоліки / І. В. Ховрак // Економіка. Фінанси. Право. - 2013. - № 4. - С. 16-20.

Конюшок Сергій Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

МЕРЕЖА ARPANET

І. Постановка проблеми

І. І. Агенство ARPA.

За наказом президента США Дуайта Ейзенхауера, директивою міністерства оборони від 7 лютого 1958 року, було створено Агенство передових дослідницьких проектів (Advanced Research Projects Agency, ARPA). Перед працівниками **ARPA** була поставлена надскладна на той час задача, пов'язана з підвищенням обороноспроможності країни. В основу даної організації були покладені такі принципи:

- маленькі розміри організації і як наслідок - велика гнучкість у вирішенні поставлених задач;

- основу технічного персоналу складали вчені і інженери із світовим іменем;

- при запуску будь-якого проекту, обов'язковою умовою було досягнення кінцевого результату і практична реалізація.

I.II. Що являє собою мережа ARPANET?

ARPANET (***Advanced Research Projects Agency Network***) – комп'ютерна мережа, створена в 1969 році в США Агентством Міністерства оборони США з перспективних досліджень (**DARPA**) і стала прототипом мережі Інтернет. 1 січня 1983 вона стала першою в світі мережею, яка перейшла на маршрутизацію пакетів даних. В якості протоколу маршрутизації використовувався **TCP/IP**, який і донині є основним протоколом передачі даних в Інтернеті.

I.III. Історія виникнення.

Перша спроба створити комп'ютерну мережу на основі методу комутації пакетів був початий в лютому 1965 р. Через час вченим Т. Мериллу і Д. Лікляйдеру вдалося зв'язати низькошвідкісною комутаційною лінією на швидкості 1200 біт/с два комп'ютери - TX-2 із MIT Lincoln Lab і AN/FSQ-32 із System Development Corporation. В кінці 1967 року ARPA заключила контракт із Стенфордським дослідницьким інститутом на розробку детальної специфікації для майбутньої комутаційної мережі. Перший сервер **ARPANET** було встановлено 1 вересня 1969 року у Каліфорнійському університеті в Лос-Анджелесі. Комп'ютер «Honeywell 516» мав 12 кілобайт оперативної пам'яті.

II. Мета роботи

Головною метою дослідження цієї теми є показ аспектів та їх розуміння і впровадження технології **ARPANET**. Розгляд способів роботи на практиці та вивчення їх можливостей. Виділення переваг та ефективності технології.

III. Мережа ARPANET

ARPANET - мережа, яку вважають початком Інтернету. Першочергове завдання — об'єднати у мережу науково-дослідницькі та військові інститути у США, задля збільшення швидкості та покращення зручності обміну інформацією між ними. В умовах Холодної війни також стояла задача створити інфраструктуру, спроможну пережити атомний удар. По замовленню **DARPA** в **BBN** почали розробку пристроїв **IMP** (**Interface Message Processor**), в задачу яких входило забезпечити зв'язок між комп'ютерами через телефонну мережу. 1 листопада і 1 грудня два **IMP**-пристрої були встановлені в Каліфорнійському університеті і в Університеті штату Юта. Через рік вузлів стало 15 і вони використовували для обміну пакетами протокол **NCP** (**Network Control Protocol**). У 1970-х роках мережа загалом використовувалась для пересилки електронної пошти, тоді ж з'явилися перші списки поштових розсилок, групи новин та дошки оголошень. Але в ті часи мережа ще не могла легко взаємодіяти

з іншими мережами, котрі були побудовані на інших технічних стандартах. До кінця 1970-х років почали активно розвиватись протоколи передачі даних, що були стандартизовані у 1982–1983 роках. 1 січня 1983 року мережа **ARPANET** перейшла з протоколу **NCP** на протокол **TCP/IP**. У 1973 році до мережі були підключені перші іноземні організації з Великобританії та Норвегії, і мережа стала міжнародною. Вартість пересилки електронного листа по мережі ARPAnet становила 50 центів. До основних характеристик мережі **ARPANET** відносять: закритість мережі, організованість за принципом Top-Down, використання поштових розсилок, (які модерувались). У 1984 році була розроблена система доменних назв (англ. Domain Name System, **DNS**). Тоді ж у мережі **ARPANET** з'явився серйозний суперник — Національний науковий фонд США (**NSF**) заснував міжуніверситетську мережу **NSFNet** (англ. National Science Foundation Network), котра була сформована з дрібніших мереж, включаючи відомі на той час **Usenet** та **Bitnet** і мала значно більшу пропускну здатність, аніж **ARPANET**. У 1990 році мережа **ARPANET** припинила своє існування, програвши конкуренцію **NSFNet.**

Висновок

Не дивлячись на величезні досягнення, самим розробникам мережі ріст **ARPANET** здавався дуже повільним. Роберт Тейлор писав: "Наша робота просувалась дуже повільно. До 1971 року в склад входило 15 вузлів, і це не дивлячись на те, що початково планувалось 30. Основна причина такого повільного росту заключалась в тому, що більшість комп'ютерів не мало єдиного програмного забезпечення". Хоча дана технологія і мала безліч недоробок, і мала погані технічні характеристики, але вона дала величезний поштовх у розробку і заснування інтернету такого, яким ми його бачимо зараз. Я вважаю, що завдяки цій технології і пішов науковий прогрес в сфері передачі інформації і побудові телекомунікаційної мережі.

Література:

1. Wikipedia [Електронний ресурс] // Інтернет - Режим доступу: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82; 2. Wikipedia [Електронний ресурс] // Aspen Movie Map - Режим доступу: https://uk.wikipedia.org/wiki/ARPANET;
2. Виртуалный компютерный музей [Електронний ресурс] // Создание сети ARPANET - Режим доступу: http://www.computer-museum.ru/connect/arpanet.htm;
3. WORLD of SCIENCE and TECHNOLOGIES [Електронний ресурс] // Що таке ARPANET або історія створення сучасного інтернету - Режим доступу: http://scitechspace.blogspot.com/2015/03/arpanet.html;
4. Освіта [Електронний ресурс] // История развития Интернета. 1961-1970 гг. ARPANET. IMP. NCP - Режим доступу: https://stwat2343.wordpress.com

Мірошник Валерія Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРША У СВІТІ ФОТОННА НЕЙРОННА МЕРЕЖА

У роботі були представлені результати досліджень вчених, щодо вивчення нової фотонної нейронної мережі у світі ІТ технологій, яка була досліженням вчених Прінстонського університету.

Нейромережі беруть штурмом світ обчислень.

Дослідники використовують їх для створення машин, здатних виконувати дії, які раніше вважалися винятковою прерогативою людини - розпізнавання образів, осіб, обробка природних мов. Ці та інші навички вже зараз виконуються машинами абсолютно однаково.

Дослідники Прінстонського університету займаються побудовою схем нового проекту.

Одним з напрямків в цій роботі є конструювання схем, ланцюгів, які за своєю архітектурою функціонуватимуть подібно нейронам - так званих нейроморфних чіпів

Представлення інтегральної мікросхеми з кремнію.

Фотонний нейроморфний чіп, здатний проводити обчислення на шалених швидкостях.

Оптичні комп'ютери давно вважаються обчислювальними машинами майбутнього: діапазон оброблюваних частот у фотонів значно вище, ніж у електронів, тому вони обробляють дані набагато швидше. Однак вартість таких пристроїв завжди була неприпустимо велика.

Нейронні мережі відкрили фотоніці нові можливості.

Першим кроком в цьому напрямку стала розробка оптичного пристрою, де у кожного вузла така ж частотна характеристика, як у нейрона. Ці вузли є мініатюрними круглі хвилеводи, вирізані на кремнієвій підкладці, де циркулює світло. Той же світло виступає сигналом на введенні для лазера і регулює його вихідну потужність.

Вчені виміряли вихідний сигнал і з'ясували, що математично він еквівалентний безперервно-часової рекурентної нейронної мережі.

Важливо, що кожен вузол системи налаштований на конкретну довжину хвилі (ця техніка називається хвильовим мультиплексуванням).

Потім сигнал лазера знову потрапляє в вузли, що створює нелінійну систему зворотного зв'язку.

Важливість цього результату в тому, що новий пристрій вже може користуватися безліччю програмних засобів, створених для такого роду нейронних мереж.

На прикладі мережі з 49 фотонних вузлів дослідники емулювали одне диференціальне рівняння і показали, що фотонна нейронна мережа

справляється із завданням приблизно на три порядки швидше, ніж звичайний центральний процесор.

Література:

1) http://tech.obozrevatel.com/digest/70194-amerikanskie-uchyonyie-razrabotali-pervuyu-v-mire-fotonnuyu-nejronnuyu-set.htm;
2) https://hightech.fm/2016/11/23/silicon-photonic-neural-network;
3) https://indicator.ru/news/2016/11/21/sozdana-pervaya-v-mire-fotonnaya-nejronnaya-set/;
4) http://22century.ru/chemistry-physics-matter/37824.

Васильчук Яна Олександрівна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПОКОЛІНЬ МОБІЛЬНИХ МЕРЕЖ ВІД 1G ДО 5G

Кожні 10 років з'являються нові покоління мобільних мереж зі своїми особливостями, принципами побудови, та найголовніше – з новими послугами. Існує безліч різних мобільних стандартів, які постійно змінюються та вдосконалюються. Для спеціаліста з телекомунікацій дуже важливо орієнтуватися і знати особливості технологій мобільного зв'язку. Розглянемо еволюцію поколінь мобільних мереж та їх основні характеристики.

Покоління стільникового зв'язку - це набір функціональних можливостей роботи мережі, а саме: реєстрація абонента, встановлення виклику, передача інформації між мобільним телефоном і базовою станцією по радіоканалу, процедура встановлення виклику між абонентами, шифрування, роумінг в інших мережах, а також набір послуг, що надаються абоненту.

Еволюція систем стільникового зв'язку включає в себе кілька поколінь 1G, 2G, 3G і 4G. Ведуться роботи в області створення мереж мобільного зв'язку нового п'ятого покоління (5G).

Комерційну реалізацію мобільна телефонія отримала в 1984 році у вигляді мобільних мереж першого покоління (1G), які були засновані на аналоговому способі передачі інформації. Основними стандартами аналогового мобільного зв'язку стали AMPS (Advanced Mobile Phone Service), TACS (Total Access Communications System), NMT (Nordic Mobile Telephone). Вище перелічені стандарти використовувалися лише для голосової передачі даних. Фактично в кожній країні була власна система, незалежна від систем та обладнання інших країн. Так виникла потреба створити спільну систему з високою пропускною можливістю та широкою зоною покриття.

В 1982 році європейська конференція поштових та телекомунікаційних відомств CEPT (Conference of European Post and Telecommunications) сформувала спеціальну групу для вивчення та розробки наземної системи безпроводового зв'язку загального користування GSM (Groupe Spécial Mobile).

Так на світ з’явилося друге покоління – 2G. Основною відмінністю між 1G та 2G став цифровий спосіб передачі даних. Всі телефонні розмови були зашифровані з допомогою цифрового коду. Також на світ з’явилася всіма улюблена послуга SMS (Short Message Service).

Представниками другого покоління, окрім GSM, є стандарти D-AMPS (Digital AMPS) та CDMA (Code Division Maltiple Access). Потім з’являється технологія GPRS (General Packet Radio Service), яку називають технологією покоління 2.5G. GPRS використовує принцип розподілення каналів для передавання голосового трафіку й трафіку даних, а також забезпечує можливість прийому під час GPRS-з'єднання як телефонних дзвінків, так і SMS-повідомлень. Додатково оператори пропонують послуги мультимедійних MMS повідомлень. Користувачі мобільних телефонів можуть мати також доступ в Інтернет. Однак швидкість такого доступу є невисокою (2 400 – 9800 Кбіт/с). [4]

Пакетна передача даних дозволила збільшити швидкість передачі інформації під час роботи мобільного пристрою з Інтернетом з 9,6 кбіт/с до 384 кбіт/с. Технології GPRS та EDGE вже неможливо було назвати 2G, оскільки вони були набагато швидші, ніж друге покоління, але в той же час не дотягували до третього. Доволі часто GPRS називали поколінням 2,5G, а EDGE – 2,75G.

Подальшим розвитком мереж мобільного зв'язку став перехід до третього покоління (3G). 3G - це стандарт мобільного цифрового зв'язку, який під абревіатурою IMT-2000, об'єднує п'ять стандартів - W-CDMA , CDMA2000, TD-CDMA / TD-SCDMA, DECT (Digital Enhanced Cordless Telecommunication).

Стандарт IMT-2000 дає чітке визначення мереж 3G - під мобільного мережею третього покоління розуміється інтегрована мобільна мережа, яка забезпечує:

- для нерухомих абонентів швидкість обміну інформацією не менш 2048 кбіт/с;
- для абонентів, що рухаються зі швидкістю не більше 3 км / год - 384 кбіт/с;
- для абонентів, які переміщуються зі швидкістю не більше 120 км / ч - 144 кбіт/с.

Основою всіх стандартів третього покоління є протоколи множинного доступу з кодовим розділенням каналів.

Подальшим розвитком мереж стала технологія HSPA (High Speed Packet Access), яку стали називати 3,5G. Спочатку вона дозволяла досягти швидкості в 14,4 Мбіт / с, проте зараз теоретично досяжна швидкість 84 Мбіт / с і більше.[3]

З постійним збільшенням кількості користувачів та розвитком нових послуг, розроблені технології передачі даних для мереж 3G уже в певних випадках не можуть розв’язати поставлені перед ними завдання. Тому в 2010 році з’являється мобільна система четвертого покоління, яка працює на основі IP-мережі .

Основною метою інформаційної технології 4G є забезпечення високої швидкості передачі даних, висока якість, висока продуктивність, безпека і

низька вартість послуг передачі голосу і даних, мультимедіа та інтернет через IP. Стандарти 4G: LTE-Advanced і WiMax. Швидкості передачі: 100 Мбіт/с під час руху , 1 Гбіт/с в нерухомому стані. Сервіси, які надаються - мобільний доступ в Інтернет, IP-телефонія, ігрові сервіси, високої чіткості, мобільне телебачення, відео-конференції, 3D-телебачення, хмарні обчислення.[1,с.23-24]

5G - основа телекомунікаційної мережі, а в ідеалі, рішення майбутніх проблем, які виникнуть на моделі 4G після того, як стандарт набуде широкого застосування. Стандарт 5G - новий етап розвитку технологій, що об'єднує суспільство, який забезпечить необмежений доступ до мережі для індивідуальних користувачів і пристроїв. Вважається, що п'яте покоління мобільного зв'язку з'явиться до 2020 року.

Характеристики, які відрізнятимуть мережі п'ятого покоління від попередників[2,3]:

- швидкість від 1 до 10 Гбіт;
- збільшення пропускної здатності мережі більше 10 Гбіт/с;
- кількість одночасних підключень до 100 мільйонів пристроїв на 1 квадратний кілометр;
- забезпечення зменшення затримки в мережі до 1 мс;
- скорочення близько 90% у використанні мережевої енергії;
- термін служби батареї буде набагато довше;
- весь світ буде знаходитися в зоні Wi-Fi.

Реалізація проекту «5G до 2020 року» зробить можливим необмежений доступ до інформації. Різноманітність підключених пристроїв, додатків і завдань дозволяє припустити, що 5G стане результатом інтеграції існуючих технологій радіодоступу, як вдосконалених LTE і HSPA, так і більш спеціалізованих, спрямованих на конкретні цілі.

ЛІТЕРАТУРА

1. Тихвинский В.О. Сети мобильной связи LTE. / Тихвинский В.О., Терентьев С.В., Юрчук А.Б. – Технологии и архитектура Эко-Трендз, 2010. - 281 с.

2. Скрынников В.Г. Будущий облик 5G. – Электросвязь. № 10. – 2013.

3. Evolution of Mobile Communication from 1(G) to 4G, 5G, 6G, 7G [Електронний ресурс] // – Режим доступу: https://www.linkedin.com/pulse/evolution-mobile-communication-from-1g-4g-5g-6g-7g-pmp-cfps

4. Что такое "поколение" сетей сотовой связи? [Електронний ресурс] // – Режим доступу : http://1234g.ru/1g/chto-takoe-pokolenie-setej-sotovoj-svyazi

Сагайдак Виктор Анатолиевич
Государственный университет телекоммуникаций
Учебно-научный институт Телекоммуникаций и информатизации
г. Киев

АЛГОРИТМ МОДУЛЯЦИИ CAP

Алгоритм амплитудно-фазовой модуляции с подавлением несущей carrier (CAP) является одним из наиболее широко используемых в настоящее время на DSL-линиях методов модуляции. Алгоритм CAP представляет собой одну из разновидностей алгоритма QAM, его особенность заключается в специальной обработке модулированного информационного сигнала перед его отправкой в линию. В процессе этой обработки из спектра модулированного сигнала исключается составляющая, которая соответствует частоте несущей QAM. После того, как приемник принимает сигнал, он сначала восстанавливает несущую частоту, а после этого - поток данных. Такие манипуляции со спектром выполняются для того, чтобы уменьшить долю неинформативной составляющей в спектре передаваемого сигнала. Это, в свою очередь, делается для того, чтобы обеспечить большую дальность распространения сигнала и уменьшить уровень перекрестных помех между сигналами, которые передаются по одному кабелю.[1;2]

Из модулированного сигнала предлагается исключить именно ту гармоническую составляющую, которая должна была использоваться для переноса полезного сигнала. [1]

На рисунке синим цветом отмечен спектр передаваемого полезного сигнала. Максимальная частота этого сигнала имеет значение f_{max}. Частота модулирующего колебания-носителя имеет значение f_c. После выполнения процедуры гармонической амплитудной модуляции спектр полезного сигнала переносится в область частоты fc и приобретает зеркальные составляющие. На рисунке этот спектр помечен зеленым цветом. Для восстановления переданного сигнала на приемной стороне достаточно передать только одну из зеркальных компонент спектра модулированного сигнала. Гармоника с частотой f_c также является компонентом спектра модулированного сигнала, однако при восстановлении сигнала без неё также можно обойтись. Теоретически, амплитуда этой гармоники несет информацию об уровне постоянной составляющей передаваемого сигнала (составляющая спектра сигнала с частотой = 0). В силу этого данная гармоника не является в полной мере информативной, и её потеря не повлияет на качество восстановленного сигнала. Хотя исключение гармоники f_c из передаваемого сигнала ведет к возникновению определенных трудностей при восстановлении сигнала, эта процедура вполне оправдана, поскольку позволяет существенно снизить уровень неинформативного сигнала, передаваемого в линию. Красным цветом на рисунке показан спектр модулированного колебания, который сформирован в соответствии с принципами алгоритма CAP.[1]

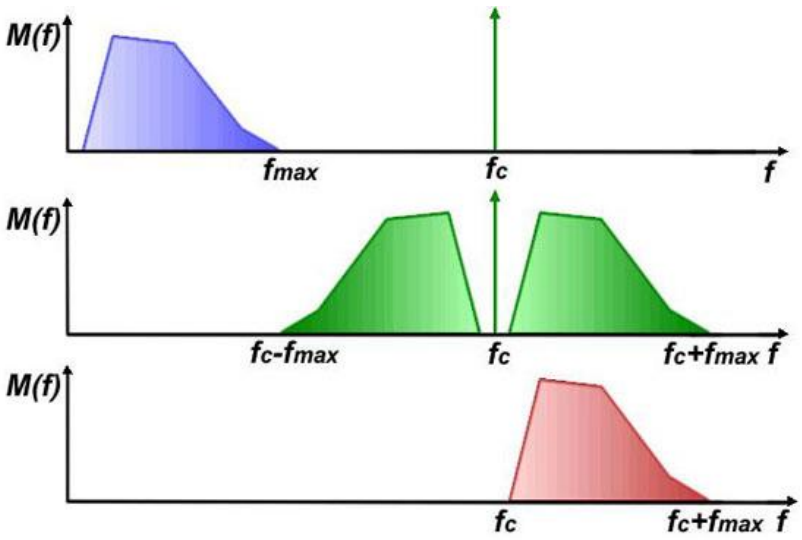


Рис. 9 Алгоритм модуляции CAP

Достоинства и недостатки алгоритма

Поскольку алгоритм амплитудно-фазовой модуляции с подавлением несущей является, по сути, алгоритмом типа QAM, ему свойственны все положительные качества, присущие этому классу алгоритмов – относительная простота реализации и высокая спектральная эффективность. Несомненным достоинством алгоритма CAP является высокая энергетическая эффективность формируемого сигнала. Именно этот алгоритм теоретически способен обеспечить максимальные значения SNR и, следовательно, передачу сигнала на наибольшие расстояния. Все эти полезные качества алгоритма модуляции CAP позволяют применять его для построения эффективных и экономичных приемо-передающих устройств широкого спектра технологий DSL - от SDSL до VDSL.[1]

Основным недостатком этого метода является отсутствие стандартизирующего документа, который определяет процедуры преобразования сигналов. Отсутствие этого документа объясняется рядом политических и экономических причин. Одной из причин, которые сдерживают внедрение этой технологии, является сильная поддержка альтернативной технологии DMT, которую оказывает комитет T1E1 ANSI. Другой причиной является недостаточная гибкость лицензионной политики, которую проводит обладатель патента на CAP - компания GlobeSpan. Эти причины, которые нельзя назвать техническими, в то же время являются достаточно вескими, для того, чтобы сдерживать процессы внедрения алгоритма CAP в перспективные системы DSL.[1]

Список источников:

1. http://www.adslclub.ru/new/02/01/08/02.html
2. http://doronin2004.narod.ru/rez_dr/bocheluk_su31/tema3_2.html

Кравченко В.А.
Таврический государственный агротехнологический университет,
Факультет инженерии и компьютерных технологий
г. Мелитополь

ГЕНЕРАЦИЯ КОДА НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ C# «НА ЛЕТУ»

Аннотация – робота посвящена исследованию возможностей метода динамической (во время выполнения приложения) генерации и запуска программного кода на языке программирования C# на примере решения нелинейного уравнения методом хорд.

На сегодня существует несколько вариантов толкования термина «искусственный интеллект», причем большинства из них существенно различается даже у представителей смежных профессий. В частности, практические программисты, в некоторых случаях, подразумевают под этим понятием программу, способную переписывать (модифицировать) саму себя. То есть, при необходимости и в зависимости от требований пользователя или решаемой задачи, приложение будет менять отдельные части собственного программного кода, подстраиваясь под новые требования.

Уже сейчас существует ряд инструментов, с помощью которых можно попытаться реализовать такую систему. Один из самых мощных – динамическая генерация кода, которую постепенно начинают применять в создании отдельных программных продуктов. Конечно, возможности такого подхода достаточно широки, однако прежде чем приступить к созданию масштабной системы, способной модифицировать саму себя и учиться таким образом, необходимо детально выучить особенности методов автоматической генерации программного кода на более простых случаях.

Одним из наиболее подходящих для решения подобных задач является объектно-ориентированный язык программирования C#. Он был создан в компании Microsoft как язык разработки приложений для платформы Microsoft .NET Framework [1, с 14]. Одной из особенностей C # является то, что приложения .NET не интерпретируются, а компилируются. Интерпретация предполагает последовательное выполнение инструкций, без предварительного их превращения в код, приемлемый для процессора и операционной системы, как это делается при компиляции. В .NET промежуточный язык не интерпретируется, а компилируется в код по мере необходимости, так что неиспользуемые функции при этом не будут даже скомпилированы. Соответственно, в C# нет и не может быть инструментов, способных в процессе работы выполнить посторонний код, как это делается, например, в языке JavaScript с помощью функции eval. Здесь всё, что будет выполняться приложением должно уже находиться в его программном коде.

Поэтому возникает необходимость разработки приложения, способного распознать и выполнить сторонний программный код без перезапуска программы. Один из возможных вариантов решения этой задачи - применение

методов автоматической генерации кода. То есть, еще на этапе разработки, в приложении прописывается шаблон, содержащий базовую структуру кода (например, объявление библиотек), в который в дальнейшем будет включено тело функции, введенной пользователем через интерфейс и который будет запущен и выполнен уже в модифицированном виде.

При этом написание программы необходимо выполнить, учитывая специфику предметной области. Например, для решения нелинейных уравнений с помощью метода хорд определяется приближенное значения корня уравнения итерационным путем, причем на каждой итерации программа работает с определенной функцией, введенной пользователем с клавиатуры уже после запуска программы. Поскольку интегрировать эту функцию в уже запущенный и работающий код напрямую невозможно, возникает необходимость динамического запуска параллельного модуля, в который формула подставляется «на лету».

Таким образом, последовательность работы программы следующая. Пользователь вводит строку, содержащую нелинейное уравнение, приближенное значение корня которого необходимо определить. После нажатия соответствующей кнопки производится динамическая генерация кода на основе уже записанного в программе шаблона (объявление библиотек и базовая структура программного кода), в который подставляется введённое пользователем уравнение, компиляция и выполнение созданного приложения. Результаты возвращаются к основной программе в виде отчета о выполнении функции из динамически сформированного кода и выводятся на экран в удобном для пользователя виде. Соответственно для этого необходимо, чтобы функция, в теле которой выполнялось вычисление корня уравнения, возвращала определенное значение, то есть была типа, отличного от void.

Ключевым моментом является использование CodeDOM – сложной совокупности классов, обеспечивающей возможность использования динамической генерации кода [2, с 15]. CodeDOM содержит типы, представляющие многие общие типы элементов исходного кода. С его помощью можно разработать программу, которая будет строить модель исходного кода, используя элементы CodeDOM для создания графа объектов. Этот объектный граф может быть выражающийся в виде исходного кода с помощью генератора кода для поддерживаемого языка программирования. Данный инструмент можно также использовать для компиляции исходного кода в двоичную сборку.

В данном случае исходный код программы, запускаемой динамично, сохраняется в отдельной текстовой строке. Инициализируя новый объект класса CompilerParameters (с указанием, что создаваемая программа будет запускаться только в пределах оперативной памяти, не имея обмена информацией с жёстким диском), получаем доступ к компилятору C# в режиме реального времени, а через объект класса CSharpCodeProvider – структурированные результаты.

Література:
1. Троелсен Э. Язык программирования C# 2005 и платформа .NET 2.0. 3-е издания / Э. Троелсен. – М.: Вильямс, 2007. – 795 с.
2. Hazzard K. Metaprogramming in .NET / K. Hazzard, J. Bock. – Manning, 2012. – 360 p.

Нідзельська Анастасія Русланівна
Державний університет телекомунікацій
факультет Інформаційних технологій
м. Київ

ЗАСТОСУВАННЯ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ В ОБРОБЦІ СИГНАЛІВ

Термін вейвлет перетворення з'явився у 80-х роках минулого сторіччя та був введений у вживання Госсманом та Морле, які досліджували властивості сейсмічних та акустичних сигналів. Наразі вейвлет перетворення широко використовуються для вирішення задач з розпізнавання образів; при обробці та синтезі різноманітних сигналів; для вивчення властивостей турбулентних потоків; для пакування великих обсягів інформації та в багатьох інших випадках. Вейвлет перетворення одномірного сигналу складається з його розкладу по базису, що сконструйовано з функції, яка має певні властивості, - вейвлета, за допомогою масштабних змін та переносів. Кожна з функцій цього базису одночасно характеризує як певну просторову (часову) частоту, так і її локалізацію у фізичному просторі (часі). Отже, на відміну від перетворення Фур'є, вейвлет перетворення забезпечує двовимірну розгортку одновимірного сигналу, що досліджується. При цьому частота та координата розглядаються як незалежні змінні. Внаслідок цього з'являється можливість аналізувати властивості сигналу одночасно у фізичному (час, координата) та в частотному просторі. В основу математичного апарату вейвлет перетворення покладено перетворення Хаара, згідно якого сигнал можна охарактеризувати його середнім значенням та його змінами відносно цього значення – флуктуаціями.

Для представлення сигналу потрібно мати одну функцію - *материнський* вейвлет (ψ). Так як материнський вейвлет має дуже швидке загасання, то для того, щоб покрити всю множину, розкладену на елементарні вейвлети приймають можливі зсуви його по осі часу. Крім цього вейвлети потрібно масштабувати по довжині.

В результаті приходимо до вейвлетів, які сформовані з одно материнського вейвлета за рахунок операцій зсуву в часі і зміни часового масштабу:

$$\psi_{ab}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right)$$

Множник $\frac{1}{\sqrt{|a|}}$ забезпечує незалежність норми цих сигналів від масштабуючого числа ***a*** .

Вейвлети характеризуються своїми часовими і частотними образами. Тимчасовий образ визначається деякою ψ (t) - функцією, а частотний задається її фур'є-образом ψ (ω), який задає огинаючу спектра вейвлета. В основі безперервного вейвлет перетворення лежить використання двох безперервних і інтегрованих по всій числовій осі t або x функцій:

- $\Psi(t)$ з нульовим значенням інтеграла $\int_{-\infty}^{\infty} \Psi(t)dt = 0$, що визначає деталі сигналу і породжує деталізують коефіцієнти;
- $\varphi(t)$ масштабуюча (або скейлінг-функція) з одиничним значенням інтеграла $\int_{-\infty}^{\infty} \varphi(t)dt = 1$, яка визначає грубе наближення (апроксимацію) сигналу і

породжує коефіцієнти апроксимації (ортогональні вейвлети). Існує кілька підходів до визначення вейвлета: через масштабний фільтр, масштабну функцію, вейвлет-функцію. Вейвлети можуть бути ортогональними, напівортогональними, біортогональних.

При числовій реалізації вейвлетного перетворення для сигналу, заданого в вигляді індексованої функції X_k, формула записується в вигляді суми:

$$W(a,b) = \frac{1}{\sqrt{a}} \sum_{k=1}^{K} X_k \psi\left(\frac{k-b}{a}\right).$$

На практиці розрахунки на основі такого виразу не є оптимальними з точки зору витрат машинного часу. Процес розрахунку може бути суттєво прискорений, якщо перейти до Фур'є-образів заданого сигналу $X_k(\omega)$ і вейвлетної-функції ψ (ω).

Література:

1. Дремин И.М., Иванов О.В., Нечитайло В.А. Вейвлеты и их использование // Успехи физических наук. – 2001. – том 171. – № 5 –С.465-501.
2. http://pbf.kpi.ua/txt/pbf/Vistnik/35/Part_3.pdf
3. Вычислительные методы и программирование, 2001, Т. 2: Переберин А. В. О систематизации вейвлет-преобразований

Щербина Віктор Володимирович, аспірант
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
кафедра Менеджменту
м. Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК КОНКУРЕНТНА ПЕРЕВАГА ПІДПРИЄМСТВ

Нині невеликі і середні роздрібні мережі зазнають усе більш сильного тиску з боку великих підприємств. Планувати подальший розвиток можна тільки забезпечивши підвищення ефективності бізнесу, що неможливо без впровадження багатофункціональних і надійних інформаційних систем, що дозволяють управляти роздрібною структурою, логістикою, асортиментом, цінами. Сучасні інформаційні системи надають можливість обробляти значну кількість інформації, взаємодіяти з підрозділами підприємства, збільшувати швидкість і якість обслуговування клієнтів.

Виклад основного матеріалу: Домінуючим напрямом зараз є широке впровадження інформаційно-аналітичних систем для вирішення завдань прогнозування попиту, планування закупівель, управління запасами, ефективного мерчандайзинга і тому подібне. Впровадження інформаційних технологій (ІТ) пов'язане з:

1) технологічною необхідністю - коли використання ІТ диктується вимогою забезпечення складних технологічних операцій (наприклад, обробки штрихових кодів).

2) потребою в засобах аналізу ефективності - за наявності великого числа однорідних "виробничих ділянок" (філії, менеджери по продажах і т. д.), результати діяльності яких можна і треба постійно зіставляти.

Існує п'ять головних причин складності впровадження і використання інформаційних систем на підприємствах роздрібної торгівлі :

поверхневе розуміння концепції керівництвом компанії; недостатній рівень розвитку ІТ-інфраструктури торговельного підприємства; низька кваліфікація консультантів компании-внедренца;

помилки при виборі автоматизованої системи і опір персоналу самого торговельного підприємства.

Підприємства роздрібної торгівлі виявляють цікавість до наступних областей інформатизації :

1) системи аналізу даних - BI для обробки значної кількості інформації з більшою швидкістю, які дозволяють швидко отримувати звідні дані про ефективність роботи усього підприємства (наприклад, систему класу SAP, Microsoft Dynamics AX, Oracle BI), аналізувати усю інформацію, наявну в торговельній організації, незалежно від того, в якій інформаційній системі вона накопичується. Основою цього рішення є сховище даних, яке акумулює інформацію з різних джерел і, завдяки спеціальній структурі, дозволяє формувати звіти набагато швидше, ніж в ERP -системах.

2) системи управління стосунками з клієнтами - CRM. В умовах зростаючої конкуренції усе більше число торговельних підприємств зацікавлене в тому, щоб краще знати своїх покупців і ефективніше здійснювати політику в області асортименту, маркетингу і управління скидками. Окрім CRM -систем це різні IT-продукти для взаємодії з клієнтом через SMS і спеціалізовані програми для роботи з бонусними картами.

3) системи управління мережами магазинів (SCM), які залишаються затребуваними торговельними компаніями (наприклад, Visual Pos Manager (VPM), що дозволяє з єдиного центру управляти усіма касами і скидками роздрібної мережі, і який інтегрується з SAP Retail, Microsoft Dynamics AX, 1C, Oracle Retail і так далі). Конкурентні переваги: функціональність, надійність, і відпрацьовані технології впровадження, супроводу і навчання користувачів.

4) робочі місця касирів - PosX, оснащені касовою програмою, адже окрім стандартних операцій по прийому грошей і видачі здачі, вимагається організувати прийом безготівкових платежів, обслуговування дисконтних і бонусних карт.

5) програма "1 С: Роздріб 8" на платформі "1 С: Підприємство 8" - підтримує роботу з територіально розподіленими інформаційними базами (РІБ). При цьому забезпечується чіткий розподіл документообігу по магазинах, а в центральному вузлі РІБ консолідується інформація по усіх магазинах мережі. В результаті усі процеси, що вимагають інформаційного обміну, проводяться не лише з мінімальними трудовитратами, але і відповідно до регламенту, а центр оперативно отримує необхідну для ухвалення управлінських рішень інформацію про продажі і рух товару

6) використання кишенькових комп'ютерів або комунікаторів (КПК) - тобто мобільної торгівлі, системи RFID. Ці пристрої виступають сховищем інформації про клієнтів, товар, розрахунки і служать для занесення інформації про продажі. Дані регулярно синхронізуються з основною обліковою системою підприємства. Система підвищує оперативність роботи торговельних агентів і економить їх час для безпосереднього спілкування з клієнтами.

Висновки: Таким чином, застосування інформаційних технологій в роздрібній торгівлі багато в чому зумовлює успішність розвитку торговельної організації. Інформаційні продукти покликані спрощувати і удосконалювати систему контролю оперативної діяльності компанії (фінанси і витрати, запаси і склад, закупівлі і продажі, дебіторська заборгованість і цінова політика), управляти взаєминами із замовниками і постачальниками, контролювати процес продажів. Якщо раніше на ринку пропонувалися рішення, доступні за ціною тільки великим компаніям, то останніми роками з'явилися повноцінні автоматизовані системи мобільної торгівлі, доступні навіть малим підприємствам. На сучасному ринку зберегти конкурентні позиції вдається тільки тим, хто постійно розвивається і використовує нові технології.

Література:

1. www. 1C39.ru
2. www.salespro.ru
3. www.cnews.ru
4. Бурмин А.А. "Использование программного обеспечения на предприятии"// Корпоративные системы. - 2006. - №1. - с.56-57.
5. www.zn.ua.

Остапенко Галина Андріївна
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

FRACTAL CODING

Much attention of the scientific community and enterprises - manufacturers of digital image processing systems on the problems of creation of alternative video compression systems

- Vector coding;
- Wavelet (Wavelet) conversion;
- Fractal coding;
- Combined systems potentially provide higher compression ratios

Fractals - amazing mathematical objects, its simplicity and rich features on construction of objects of complex nature with just a few factors and a simple iterative scheme It is these features and allow you to use them for image compression, especially for nature photography and other complex self-similar images

In fractal coding, which is one of the most effective methods according to the degree of packing, the image is dividing into several units called domains. Then, in the standard implementation of the method searches for similarity to each domain regions of the same image, generally a larger size. Found these areas called rank, determine the algorithm of conversion for playback domains. Search rank areas in the standard implementation of the method is carried out by trying all possible variants, which determines a significant coding time. At the initial stage of research managed by dozens of times to reduce the time of fractal image coding, but before the implementation of the coding systems operating in real time, conduct further work is required. The achieved results can already find a use for the archiving and playback of images, taking into account their rapid iterative recovery.

Fractal image compression - Image compression algorithm with losses, based on the use of iterated function systems (usually non-affine transformations) to images. This algorithm is known that in some cases, provides a very high compression ratios (the best examples - up to 1000 times with acceptable visual quality) for the real photos of natural objects, which is not available to other image compression algorithms, in principle, due to the difficult situation with the patenting of a wide propagation algorithm is not received.

The basis of the method of fractal coding - this finding self-similar areas in the image.

The basis of the method of fractal coding - this finding self-similar sites in Iterated Function System(IFS) for image compression to image compression problem was investigated for the first time the possibility of applying the theory of Michael Barnsley And Alan Sloan (born Alan Sloan.). They patented the idea in 1990 and 1991 (U.S. Patent 5,065,447). A. Zhaken (fr. Arnaud Jacquin) presented a method of fractal coding, which uses the system domain and rank of image blocks (Eng. Domain and range subimage blocks), blocks a square shape covering the entire image. This approach became the basis for most of the fractal coding methods. It has been improved Yuval Fisher and a number of other researchers.

In accordance with this method, the image is divided into a plurality of non-overlapping Ranked sub images and is defined by a plurality of overlapping domain sub images. For each rank block, coding algorithm finds the most suitable domain block and an affine transformation that translates the domain blocks in the block of rank. The structure of the image is displayed in rank blocks, blast blocks and transformation.

The idea is as follows: Suppose that the original image is a fixed point of a contraction mapping. Then instead of the image can remember any way this mapping, and to restore it suffices to apply repeatedly mapping the start any image.

The main difficulty of fractal compression is that the exhaustive search is required to find the appropriate domain blocks. Because each time should be compared the two arrays, the operation turns out long enough. Relatively simple transformation of its operations can be reduced to the scalar product of two arrays, however, even the calculation of the scalar product requires a fairly long time.

When it is known quite a number of optimization algorithms for sorting that occurs when a fractal compression, as the majority of the articles studied the algorithm, focused on this issue during the active study (1992-1996 years) came out to 300 articles per year. The most effective were the two areas of research: the method of selection of features (feature extraction) and domain method of classification (classification of domains).

Мирошниченко Наталія
Держаний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

СОЦІАЛЬНО- ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Сфера телекомунікацій є одним із найбільш суттєвих секторів світової економіки, що динамічно розвивається та формує передумови для подальшого розвитку інформаційного суспільства. Світова телекомунікаційна сфера надає широкий спектр сучасних телекомунікаційних та інфокомунікаційних послуг, якісні характеристики яких відповідають високим потребам споживачів. При цьому розвиток сфери телекомунікацій суттєво впливає як на соціальний, так і на економічний розвиток багатьох країн. Тому дослідження питань, пов'язаних з визначенням ступеня та закономірностей впливу розвитку телекомунікацій на розвиток економічних систем, є актуальними.

Незважаючи на те, що галузь телекомунікацій та інформаційних технологій надзвичайно капітало- та науковомістка і в неї вже залучено значні суми, цих інвестицій замало, враховуючи потенціал країни. Можна говорити про два моменти, які об'єктивно пояснюють недостатній рівень інвестування в телекомунікації в Україні: незадовільне законодавче

забезпечення діяльності інвесторів та слабка державна підтримка цьому процесу

Отже, потреба України в інвестиціях та становленні сучасного зв'язку може бути забезпечена шляхом об'єднання зусиль усіх структур галузі телекомунікацій, включаючи уряд. Основою для інвестування вітчизняного та іноземного капіталу і кредитів мають стати продумане планування та тісна співпраця учасників галузі. Але відкриття ринку послуг іноземним компаніям у розвинених країнах допускається тільки за мірою достатнього його насичення послугами, що надаються національними операторами. Такий підхід дозволяє підвищити конкурентоспроможність національних операторів, підготувати їх до умов відкритого ринку та уникнути зайняття домінуючих позицій іноземними операторами.

Сьогодні, ураховуючи сучасні тенденції розвитку світової економіки, залежність відносної величини розвитку телекомунікацій і економіки на різних етапах розвитку економіки різна. До певного рівня ВВП на душу населення залежність пряма, тобто чим вище рівень ВВП на душу населення, тим вище частка телекомунікацій у ВВП. Потім залежність стає зворотною: за умови досягнення певного рівня розвитку частка телекомунікацій у ВВП починає знижуватися, що свідчить про існування граничного набору телекомунікаційних послуг, необхідного споживачеві, вартість якого не перевищує певного обсягу

Оскільки мобільний зв’язок останнім часом становить суттєву альтернативу стаціонарному зв’язку, цільність мобільної телефонії (за даними 2009 року) перебуває на межі 120%, а доходи від надання послуг мобільного зв’язку дорівнюють 65% від усіх доходів сфери зв’язку України [6], виникає необхідність урахування цього виду зв’язку за умови встановлення закономірностей та взаємозв’язків розвитку ВВП і сфери телекомунікацій. Як наслідок, постає об’єктивна необхідність перегляду пропорційно-випереджального закону та визначення сучасної закономірності, яка враховує вплив на розвиток економіки країни не тільки стаціонарного, а й мобільного зв’язку.

За останнє десятиріччя сфера зв’язку перебувала на підвищувальній хвилі інноваційного зростання, обумовленій галопуючим розвитком інноваційної технології мобільного зв’язку перших трьох поколінь. У 2008-2009 р. розпочався період насиченості телекомунікаційними послугами цих поколінь, що характеризується уповільненням темпів зростання абонентської бази операторів мобільного зв’язку

Розвиток галузі телекомунікацій визначається лібералізацією та глобалізацією ринку телекомунікації. Лібералізація зумовлена переходом від монопольної структури надання послуг до конкурентного середовища і, як наслідок, зростанням кількості операторів недержавної або змішаної форм власності та кількістю мереж, заснованих на сучасних технологіях.

Основними пріоритетами розвитку галузі зв'язку в Україні є:

- забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання;
- впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень;
- дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості

Нині ринок інформаційних і телекомунікаційних технологій - один з найбільш прибуткових секторів економіки України, що динамічно розвивається. Проте досягнутий рівень телефонізації досить низький у порівнянні з показниками розвинених країн.

Література:

•1. Латік В. Основні показники рівня життя населення // Праця і зарплата, 2005. - №10. - С.
•2. Довгаль О.Г. Соціальні послуги , як елемент ринкової інфраструктури //Формування ринкових відносин в Україні, 2003. - № 7-8.

Карпенко Марія Анатоліївна
Державний університет телекомунікацій
Факультет Інформаційних технологій
м.Київ

ПОСТРОЕНИЕ МАЛОЙ КОМПЬЮТЕРНОЙ СЕТИ

Сеть – это средство передачи даными между цифровыми устройствами. Она является неотъемлемой частью современного бизнеса, заменив собой телефон, почту, архивы и многое другое. Теперь, благодаря компьютерным сетям, мы значительно экономим время и ресурсы для обмена информацией и общения, а доступ сотрудников к документам или базам данных предприятия, а также выход в Интернет осуществляется в основном через компьютерные сети.
Локальная система (LAN, ЛВС) связывает оборудование, физически находящееся на ограниченной территории (офис, одно здание). Преимущества этой сети в совместном доступе к папкам, документам, допустим, одной фирмы или компании для всех сотрудников. На одном компьютере запускается серверная часть – требовательная к производительности, обрабатывающая большой объем информации. На других компьютерах запускаются клиентские части той же программы и обращаются к серверной части по сети. Они пользуются тем, что уже обработала для них серверная часть, и поэтому

нормально работаю даже на довольно «слабых» компьютерах. Еще одних плюс использования данной сети - это удаленное управление и удаленный доступ к рабочему столу. Пользователь одного компьютера видит на своем экране то, что происходит на другом компьютере. Соответственно, он может запускать на том компьютере программы и работать в них, изменять настройки удаленного компьютера.

Компьютерная сеть состоит из узлов (хостов) и соединяющей их среды передачи данных. Узлами являются компьютеры, маршрутизаторы, сетевые принтеры, IP-камеры, то есть любые устройства, которым может быть присвоен сетевой адрес. Средой передачи могут служить кабели (медные, оптоволокно) или радиоволны. В малых сетях обычно используют адреса из диапазона 192.168.1.2 – 192.168.1.254. Кроме IP-адресса, сетевому адаптеру назначается маска сети, в малых сетях чаще всего используется маска 255.255.255.0 .

Построение компьютерной сети для офиса, малого бизнеса начинается с сбора информации: для каких целей будет использоваться сеть, степень нагрузки на систему. Далее следует этап определение набора технических средств: выбор размера и топонимики сети, оборудования, программных средств. Потом подготовка сметы: просчет финансовых затрат, анализ эффективности проекта и согласование его стоимости с заказчиком. Далее начинается процесс подготовки рабочего проекта: создание плана разводки, схемы подключения сети.

Монтаж включает в себя следующие этапы:

- Обследование объекта и составление предварительного технического проекта и расчет сметы на оборудование и монтажные работы для **прокладки ЛВС.**
- **Монтаж кабельной трассы** включает в себя монтаж скрытой проводки, коробов, напольных и потолочных каналов, подвесных линий внутри и вне помещений, монтаж кабельных гофрированных шахт, пластиковых труб, включая трассы за гипсокартоном. Так же на данном этапе **монтажа локальных сетей**, специалисты проводят работы по трассировке кабеля (размотка, нарезка, растяжка), жгутовании и маркировке кабельной трассы, и осуществят непосредственно **прокладку кабеля** по кабельным трассам.
- Подключение существующих и планируемых рабочих мест к кабельной сети осуществляется путем подключения встраиваемых розеток в кабельные пластиковые каналы, а так же выполняется монтаж внешних и внутренних розеток на стены, монтаж стоек, башен, розеток и люков.
- Следующий этап *монтажа локальной кабельной сети* заключается в установке коммутационных шкафов и серверных комнат (коммутация узлов СКС и маркировка, монтаж кабельных желобов и монтаж

оборудования систем вентиляции, серверов и систем бесперебойного питания, а также монтаж и настройка активного и пассивного сетевого оборудования).

- Финальный этап в **монтаже ЛВС**– это сертификация и тестирование внедренного решения. **Тестирование локальной сети** проводится специалистами, после тестирования и подтверждения качества выполненных работ происходит сертификация структурированной кабельной системы (СКС) и предоставляется полный пакет документов, включая гарантийные обязательства.

Литература:

1. http://lanport.com.ua/services/id/local-network
2. http://www.sysadmin.in.ua/proektirovanie-setey/
   Информационные системы малого предприятия. Простые решения. Сенкевич Г.Е.

Цапчук Юрій
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту і підприємництва
м. Київ

СУЧАСНИЙ СТАН ТА СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ

Розвиток соціально – економічних систем привів до того, що людина дістала можливості формування в новому соціумі. Вона стає соціально – активним, суспільним суб'єктом – особою зі своїм психологічним складом, дієздатністю і роллю в суспільстві. В цих умовах важливе місце в житті людини, в її соціальній діяльності займає зв'язок. Він (зв'язок) не лише перестає бути галуззю економіки країни в системі суспільного розподілу праці, організаційних і економічних відносин, але й є безпосередньо включеним в органіку людини. "Людина як особа сама створює і будує свої відносини, бере участь у соціальному спілкуванні, управляє процесами. Зв'язок створює і матеріальні умови цього управління. За допомогою засобів зв'язку людина здійснює комунікацію як у сфері виробництва так і в соціальних відносинах. При цьому природа зв'язку проявляється передусім у характері його послуг, тобто його предмета. Саме через предмет долається простір. Зв'язок поєднує людей для спілкування...", яке є однією з найбільш важливих потреб людини.

Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися

випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.

Ці загальні закономірності повинні стати визначальними для розвитку телекомунікацій України на найближчу і більш віддалену перспективу. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

Сьогодні сфера зв'язку та інформатизації України це:

- 86 377 суб'єктів господарювання різних форм власності, що здійснюють діяльність у сфері зв'язку та інформатизації;
- 298 000 зайнятих у сфері зв'язку та інформатизації;
-13 % – відсоток працівників підприємств сфери ІКТ від середньої кількості працівників сфери послуг;
- 9 523 суб'єкти господарювання, які здійснюють діяльність у сфері ІТ;
- 4 255 операторів та провайдерів, що внесені до Реєстру операторів, провайдерів телекомунікацій;
- 2 973 оператори, що мають ліцензії на певний вид діяльності у сфері телекомунікацій;
- 2 892 суб'єкти господарювання, що надають послуги доступу до Інтернету;
- 148 вищих навчальних закладів, що здійснюють підготовку фахівців для сфери ІКТ;
- 46 967 осіб, що складають загальний ліцензований обсяг студентів для ІТ-сфери;
- 67,5 млрд грн – обсяг доходів від надання послуг сфери зв'язку та інформатизації за 2015 рік, що складає 21,5 % загальноукраїнського обсягу реалізованих послуг;
- 52,4 млрд грн – обсяг доходів від реалізації послуг зв'язку за 2014 рік (без Автономної Республіки Крим), що на 2,0 % більше за суму доходів, отриманих у 2013 році;
- 15,1 млрд грн – обсяг реалізованих послуг у сфері інформатизації за 2014 рік, що на 32,4 % більше ніж у 2013 році;
- 1,39 % – частка сфери ІТ у ВВП (1,22 % – за аналогічний період 2013 року);
- 57,1 % – відсоток регулярних користувачів мережі Інтернет;
- 39,3 % – відсоток домогосподарств, що мають широкосмуговий доступ до Інтернету;
- 20 % – відсоток домогосподарств, що мають доступ до послуг кабельного телебачення;

- 142,4 % – рівень проникнення (за даними операторів) мобільного зв'язку – майже повне покриття території країни, відсоток від загальної чисельності населення України.

Але в Україні існують і пробле у соціально-економічному відділі. Основними проблемами розвитку ринків телекомунікацій є:

- повільне впровадження на мережах рухомого (мобільного) зв'язку радіотехнологій третього та четвертого поколінь (3G, 4G) для забезпечення держави та її громадян усіма перевагами сучасних телекомунікаційних мереж та послуг;

- нерівномірність забезпечення споживачів (особливо у сільській, гірській місцевості і депресивних регіонах) телекомунікаційними послугами, у тому числі загальнодоступними та послугами ШСД до Інтернету;

- необхідність модернізації телекомунікаційних мереж фіксованого місцевого зв'язку (наявність значної кількості аналогових комутаційних станцій), впровадження процедури встановлення внутрішньозонових з'єднань із використанням семизначних зонових абонентських номерів;

- затримка із впровадженням на мережах фіксованого та рухомого (мобільного) зв'язку послуги із перенесення абонентських номерів та неможливість забезпечити реалізацію права абонентів на вільний вибір постачальників послуг у повному обсязі;

- невідповідність існуючих нормативно-правових та нормативно-технічних документів галузі сучасному стану та перспективам розвитку телекомунікаційної мережі загального користування (далі – ТМЗК) інформаційно-телекомунікаційних технологій та потребам ринку телекомунікацій України;

- втрата значного сегменту ринку телекомунікацій України внаслідок тимчасової окупації Російською Федерацією території Автономної Республіки Крим та м. Севастополь, зменшення доходів українських операторів від надання телекомунікаційних послуг та надходжень до державного бюджету;

- погіршення сталості функціонування телекомунікаційних мереж на тимчасово окупованих територіях та на території проведення антитерористичної операції, виникнення організаційних та технологічних проблем взаємодії таких мереж з іншими телекомунікаційними мережами на території України;

- необхідність збереження цілісності міжнародної структури нумерації, яка визначена рекомендаціями Міжнародного союзу електрозв'язку, Національним планом нумерації України та встановленого порядку маршрутизації трафіку голосової телефонії на ТМЗК України у зв'язку із порушенням Російською Федерацією вимог міжнародного законодавства у сфері телекомунікацій;

- порушення майнових прав суб'єктів ринку телекомунікацій України на тимчасово окупованій території, втручання у роботу телекомунікаційних мереж

загального користування, збройне захоплення об’єктів і ліній зв’язку та перешкоджання здійсненню підприємницької діяльності.

Висновки. Стрімкий розвиток сучасних телекомунікацій суттєво впливає на соціально-економічний розвиток багатьох країн, і України в тому числі. Тому в наявних наукових дослідженнях доведено залежність розвитку телекомунікаційного зв'язку та розвитку світової і національних економічних систем, сформульовано закономірність, що доводить пропорційно-випереджальне зростання галузі зв'язку стосовно економіки країни.

Незважаючи на визначений обсяг соціально-економічних проблем, сфера телекомунікацій, яка займає значне місце в економіці країни (регіону, району), чинить значний вплив на її соціально-економічний розвиток. Проблеми складні, однак без їх вирішення неможливий подальший розвиток телекомунікацій та економіки країни в цілому та її окремих регіонів.

Література:

1. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С. О. Довгий [та ін.]. – К.: Укр. видав. центр, 2002. – 520 с.

2. Системный анализ предприятий связи: учеб. пособ. / М. В. Захарченко [и др.]. – О.: УГАС, 1996. – 66 с.

3. Варакин Л. Е. Электросвязь и экономика: информационно-экономический закон / Л. Е. Варакин // Электросвязь. – 1992. – № 12. – С. 2-6.

4. Офіційний сайт Державного комітету статистики України [Електронний ресурс]. – Режим доступу: <Http://www. ukrstat. gov. ua>.

5. Инновационный менеджмент: учеб. для вузов / С. Д. Ильенкова [и др.]. – М.: Банки и биржи, ЮНИТИ, 1997. – 327 с.

Шевченко Ольга Олексіївна
Державний університет телекомунікацій
Факультет Інформаційних технологій
м. Київ

ТЕХНОЛОГІЯ NFC

Наразі існує багато різноманітних стандартів бездротової передачі інформації, більшість з них працюють на досить значних відстанях. Однак, залишається необхідність надійного обміну даними на невеликих відстанях. Одному з таких присвячена ця робота.

Near Field Communication, технологія NFC – це технологія бездротового високочастотного зв’язку малого радіусу дії, котра надає можливість обміну даними між пристроями, що знаходяться на відстані близько 10 сантиметрів.[1]

Технологія NFC є логічним послідовником технології RFID (Radio Frequency IDentification, радіочастотна ідентифікація), і її основна відмінність від останньої - обмежений радіус дії. У той час, як дистанція зчитування активних RFID-міток може досягати декількох сотень метрів, мітки NFC доступні лише в межах 5-10 сантиметрів. Робоча частота NFC-чіпів знаходиться в неліцензованому радіочастотному діапазоні ISM band, що використовується для промислових, медичних і наукових цілей, і становить 13,56 МГц, а швидкість передачі інформації може бути 106 Кбіт/сек – 848 Кбіт/сек.

NFC підтримує RFID стандарти ISO 14443 / Mifare, FeliCa і ISO / IEC 18092. Карти, виконані за стандартом ISO 14443, також називаються БСК - безконтактні смарт-карти, - саме вони використовуються в метро; для мобільних платежів і оплати квитків в громадському транспорті Китаю і Японії використовується технологія FeliCa. Як і в стандарті ISO 14443 / Mifare в NFC зв'язок підтримується за допомогою взаємної індукції рамкових антен.[2] Звідси витікає, що технологія повністю підходить під раніше сформовану інфраструктуру транспортних карт і мобільних платежів.

Основними режимами роботи NFC-приладів є:

- читання-запис – здійснюється зчитування кодів, записаних на NFC-мітку, а також запис інформації в її пам'ять;
- P2P, піринг – зв'язок та обмін інформацією між приладами, найчастіше телефонами;
- емуляція картки – NFC-прилад виступає у якості платіжної картки або пропуску.

Встановлений NFC-пристрій може функціонувати як в активному, так і в пасивному режимі. Мобільний пристрій за умовчанням знаходиться в пасивному режимі і виконує всі функції смарт-карти. Це дозволяє економити енергію батарей портативного пристрою, а також виконувати основні функції в будь-який момент, навіть коли мобільний пристрій вимкнено. «Носієм» NFC-чіпа часто є мобільний телефон, він виступає у ролі: платіжного засобу (віртуальний гаманець), засобу ідентифікації власника, ключа, бонусної карти, проїзного квитка.

Перевага NFC - це короткий час з'єднання, одна десята секунди. Крім того, у NFC менший радіус дії, що робить цей спосіб передачі інформації більш захищеним.[3]

Технологія NFC відкриває нові можливості в сфері послуг та забезпечує легкий та зрозумілий доступ до них.

Використана література:
1. [Електронний ресурс]. – Режим доступу : URL : http://nfc-ukraine.com/
2. [Електронний ресурс]. – Режим доступу : URL : http://nano-e.ucoz.ru/
3. [Електронний ресурс]. – Режим доступу : URL : https://faqhard.ru/

Касинець Наталія
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

ХЭНДОВЕР (HANDOVER)

Хэндовер (Handover) – процедура передачи активного соединения между сотами (смена абонентом канала связи во время разговора, без потери

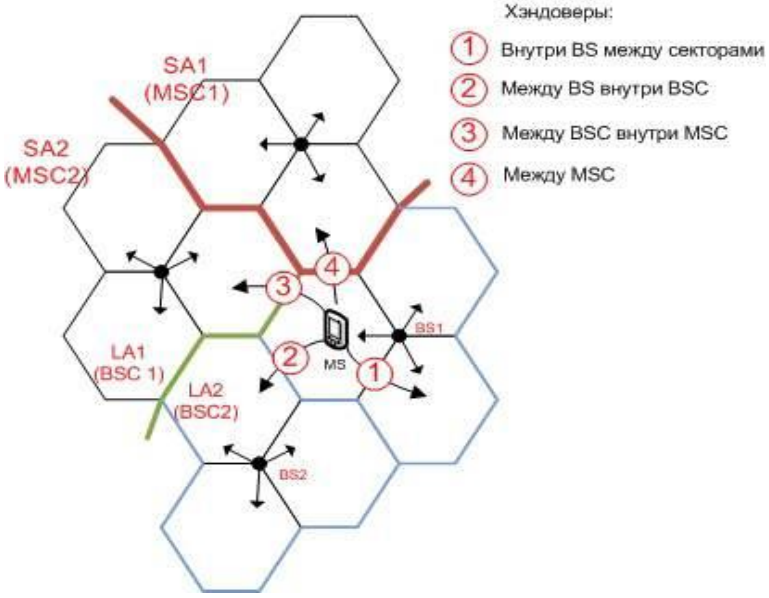
соединения). Это одна из ключевых процедур делающая сотовую связь любого стандарта (NMT, GSM, UMTS, LTE, WIMAX) истинно мобильным видом связи. Хэндовер позволяет абонентам не быть привязанным к какой-либо географической точке и дает возможность передвигаться в пределах сети оператора без разрыва соединения. Причиной хэндоверу может быть не только перемещение абонента в пространстве, но и ухудшение качества сигнала от текущей базовой станции по каким-либо другим признакам. В частности между абонентом и БС(базовая станция сетей 1G и 2G) может возникнуть препятствие, ухудшиться метеоусловия, обслуживающая базовая станция или ее часть может выйти из строя и т.п.

Кроме того, хэндовер происходит при резком ухудшении качества предоставляемого сектором сервиса, либо при слишком большом удалении абонента от базовой станции. Это «вынужденный» хэндовер.

В некоторых случаях хэндовер используется для перераспределения нагрузки между соседними секторами. Если сектор, обслуживающий абонента, перегружен трафиком, то мобильная станция может быть переключена на соседний, менее загруженный сектор с приемлемым качеством соединения.

Различают несколько типов GSM-хэндовера:

- intra-cell handover – внутри сектора;
- intra-BSC handover – между секторами, контролируемыми одним BSC;
- inter-BSC handover – между секторами, контролируемыми разными BSC, но в пределах одного коммутатора (MSC);
- inter-MSC handover –между секторами, находящимися в зоне обслуживания разных MSC



Не зависимо от типа к хэндоверу предъявляется главное правило – он должен быть незаметен абоненту и не влиять на качество соединения.

Принцип действия

Процесс передачи сессии может быть инициирован при переходе пользователя из зоны покрытия одной ячейки в зону покрытия другой. В случае использования традиционного метода "жёсткого" хендовера соединение с текущей ячейкой прерывается, после чего создаётся соединение с новой ячейкой. Этот метод известен как "break-before-make" (рус. Разрыв перед соединением) хендовер. Так как все ячейки в CDMA используют общие частоты, возможно создание соединения с новой ячейкой без прерывания соединения с предыдущей. Мягкие хендоверы требуют меньших мощностей, что уменьшает интерференцию и увеличивает возможности нагрузки. Мобильный телефон может также быть соединён с несколькими BTS. "Более мягкий" хендовер - частный случай мягкого хендовера, в котором радиосвязи, добавленные и удалённые одному и тому же узлу B.

Література:

1. http://celnet.ru/HO.php
2. https://ru.wikipedia.org/wiki

Бостанова Эльвира Олеговна
Государственный университет телекоммуникации,
факультет Информационных технологий
г. Киев

OFDM

OFDM — ортогональное частотное разделение каналов с мультиплексированием)

Это схема модуляции, использующая множество несущих. Канал делится на несколько субканалов или subcarrier (русский аналог «поднесущая» кажется мне немного смешным, я постараюсь избегать этого слова, употребляя где необходимо «вспомогательная несущая»)

В OFDM высокоскоростной поток данных конвертируется в несколько параллельных битовых потоков меньшей скорости, каждый из которых модулируется своей отдельной несущей.

Все это множество несущих передается одновременно.

Главное преимущество OFDM заключается в том, что продолжительность символа во вспомогательной несущей значительно больше в сравнении с

задержкой распространения, чем в традиционных схемах модуляции. Это делает OFDM гораздо устойчивее к межсимвольной интерференции (ISI, intersymbol interference).

Принцип работы данного метода основан на разбиении потока данных с помощью инверсного дискретного преобразования Фурье на более мелкие составляющие, которые передаются параллельно, каждый на своей частоте. Это позволяет не только добиться высокой скорости передачи данных, но и свести к минимуму разного рода помехи, особенно в виде отображенного сигнала (сигнал, отбиваемый от препятствий, которые стоят на пути его прямого следования). За счет частично перекрывающихся каналов передаваемый код получается избыточным, что может использоваться для восстановления утерянных частей.

Чтобы увидеть, как работает OFDM, необходимо смотреть на приемнике. Это действует как банк демодуляторов, переводя каждый носитель вплоть до постоянного тока. Результирующий сигнал интегрируется в течение периода символа, чтобы восстановить данные из этого носителя. То же демодулятор также демодулирует другие носители. В качестве разноса несущих равной обратному периода символа означает, что они будут иметь целый ряд циклов в периоде символа, и их вклад будет равна нулю - другими словами, не существует никакого вмешательства вклада.

Данные о OFDM

Данные, которые должны быть переданы по сигналу OFDM распределены по носителям сигнала, причем каждый носитель принимает часть полезной нагрузки. Это снижает скорость передачи данных, принимаемых каждым носителем. Чем ниже скорость передачи данных, имеет то преимущество, что помехи от отражений менее критичен. Это достигается за счет добавления времени защитной полосы или защитный интервал в систему. Это гарантирует, что данные только пробы, когда сигнал является стабильным и никаких новых Задержанные сигналы не прибывают, что приведет к изменению времени и фазы сигналаOFDM преимущества

Иммунитет к селективным замиранием: Одно из главных преимуществ OFDM является то, что является более устойчивой к частотно-селективным замиранием, чем систем с одной несущей, так как она делит общий канал на множество узкополосных сигналов, на которые воздействуют по отдельности, как равномерное затухание подканалов.

Устойчивость к помехам: Помехи, появляющиеся на канале может быть ограничена пропускной способностью, и таким образом не будет влиять на все подканалы. Это означает, что не теряется все данные.

Эффективность использования спектра: Использование близком расстоянии друг от друга перекрывающихся поднесущих, существенным преимуществом

является то, что OFDM, это обеспечивает эффективное использование доступного спектра.

Эластичные к ISI: Еще одним преимуществом является то, что OFDM является очень устойчивыми к межсимвольной интерференции и межкадрового. Это связано с низкой скоростью передачи данных по каждому из подканалов.

Эластичные эффекты узкополосных: Использование адекватного канального кодирования и перемежения можно восстановить символы, утраченных в результате частотной селективности канала и узкой полосы интерференции. Не все данные будут потеряны.

Simpler канал уравнивания: Одна из проблем, с системами CDMA была сложность канала выравнивания, которая должна была быть применена по всему каналу. Преимуществом OFDM является то, что с помощью нескольких подканалов, уравнительный канал становится намного проще.

- *Владимир Лебедев* Модуляция OFDM в радиосвязи // Радиолюбитель. — 2008. — № 9. — С. 36—40.
- *Бакулин М. Г., Крейнделин В. Б., Шлома А. М., Шумов А. П.* Технология OFDM. Учебное пособие для вузов. — М.: Горячая линия - Телеком, 2015. — 360 с. — ISBN 978-5-9912-0549-8.

Ставицкая Юлия Владимировна

Государственный университет телекоммуникации,

факультет Информационных технологий

г. Киев

BLUETOOTH 5.0

Группа сотрудников, ответственная за развитие Bluetooth объявила о том, что пятая версия технологии беспроводной передачи данных будет представлена уже 16 июня 2016 года. Через некоторое время после этого Bluetooth 5.0 будет использоваться в смартфонах, планшетах, ноутбуках и прочих устройствах.

Технологию Bluetooth начали разрабатывать в 1994 году в качестве беспроводной замены кабелям RS-232. Это была Ericsson, и шведские корни компании повлияли на название и логотип: BlueTooth произошло от имени Харальда I Синезубого, а логотип складывается из двух скандинавских рун «хаглаз» ᚼ и «беркана» ᛒ. Датский король удостоился такой чести благодаря своему второму прозвищу — «Объединитель».

Bluetooth используют для передачи данных между персональными компьютерами и периферийными устройствами, игровыми приставками и джойстиками, между телефонами и гарнитурами, наушниками, умными устройствами. Использование Bluetooth привело к тому, что сейчас в России есть целое поколение людей, помнящих, как в школе они передавали музыку и

картинки с телефона на телефон.

Технология завязана на использовании радиоволн в ISM-диапазоне (Industry, Science and Medicine), она использует свободный от лицензирования диапазон 2,4-2,4835 ГГц, и в нём применяется метод расширения спектра со скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS). Благодаря псевдослучайной последовательности переключения между частотами возможна работа нескольких устройств друг рядом с другом без помех.

Первая версия Bluetooth 1.0 была готова в 1998 году, но проблемой была плохая совместимость между продуктами различных производителей. Версия 1.1 исправила ряд ошибок и получила индикацию мощности принимаемого сигнала. Проблему с совместимостью решила стандартизация версии Bluetooth 1.2 рабочей группой IEEE. Скорость версии 2.0, выпущенной в 2004 году, достигала 2,1 Мбит/с благодаря технологии ускорения передачи данных Enhanced Data Rate (EDR), а базовая скорость составляла 1.1 Мбит/с. В 2007 году 2.1 мог запрашивать характеристики устройства для фильтрации при сопряжении и экономить батарею. Bluetooth 3.0 с технологией HS в 2009 году мог в теории разогнаться до 24 Мбит/с.

До последнего момента передовой версией была Bluetooth 4.2. Множество носимых устройств без поддержки смартфоном этой версии просто не будут работать. На смену 4.2 приходит Bluetooth 5. ArsTechnica со ссылкой на письмо исполнительного директора Bluetooth SIG Марка Пауэлла пишет о том, что скорость нового стандарта по сравнению с 4.2 увеличится в 2 раза, радиус действия — в 4 раза, а также даст «значительно больше возможностей для широковещательных пакетов». На момент написания статьи само письмо было недоступно. Уже сейчас в версии 4.2 такие пакеты имеют размер 47 байт, из которых 31 доступны для записи данных. Пока неизвестно, насколько больше они станут в новой версии.

Возможность передавать пакеты неопределенным адресатам без установки соединения широко используется так называемыми "маячками" — миниатюрными передатчиками, которые периодически передают широковещательные пакеты, которые могут содержать информацию о местоположении, заменяя систему GPS внутри зданий, рекламу и другие привязанные к локальному местоположению данные, например, информацию об экспонатах выставки.

Вот 5 фактов, которые нужно знать о Bluetooth 5.0

1. В два раза быстрее

Новая версия стандарта будет в два раза быстрее, чем Bluetooth 4.2. Таким образом, в результате несложных вычислений, получаем, что скорость передачи данных в версии 5.0 будет около 2 Мбит/с. 2.2.

2. Увеличен радиус действия

Одним из самых важных улучшений является увеличенный радиус действия. Теперь, соединять устройства по Bluetooth 5.0 можно в радиусе до 300 метров. Конечно, достичь такой цифры получится только в идеальных условиях, без преград и препятствий.

3. Функции навигации

В новую версию собираются добавить навигационные функции, что позволит использовать устройства в качестве маяков. Например, благодаря этой возможности, можно будет найти конкретный магазин в торговом центре, или отыскать человека в толпе, обнаружив его “смартфон-маячок”.

4. Готовность к Интернету вещей

Стандарт 5.0 будет оптимизирован для использования в комплектах умных домов. В частности, будет улучшена производительность и снижено энергопотребление.

5. Могут потребоваться новые устройства

Есть вероятность, что Bluetooth 5.0 не будет работать на существующих устройствах и для его функционирования потребуются новые чипы. В связи с этим, первые смартфоны и планшеты с новым Bluetooth появятся не раньше 2017 года.

Комашко А.С.
Держаний університет телекомунікацій
факультет Телекомунікацій
м. Київ

ТЕХНОЛОГІЇ ДЛЯ РАДІОІНТЕРФЕЙСА 5G

• SCMA (Sparse Code Multiple Access) - поділ абонентів на базі розрідженого коду, при цьому немає необхідності в підтвердженні про доставку. У цій технології бітові потоки різних користувачів в одному частотному ресурсі, безпосередньо перетворюються в кодове слово за допомогою так званої кодової книги з певного набору. Ці коди умовно називаються квазіортогональними і кількість цих кодів досить велика, і має двомірну структуру. Тобто вихідний сигнал накладається на кодову книгу і вже перетворений сигнал потрапляє на радіоінтерфейс. Відновлення сигналу на приймальній стороні також проводиться по кодовій книзі.

• F-OFDM (Flexibel OFDM) - вдосконалена технологія OFDM дозволяє організувати гнучке розбиття на піднесучі, гнучка зміна довжини символів і гнучка зміна циклічного префікса. Тобто під кожну задачу буде використовуватися свій набір параметрів.

• Polar Code - лінійний коригувальний код, заснований на явищі поляризації каналу. Є першим відомим кодом з субквадратичною складністю кодування і декодування, який доказово досягає пропускної здатності дискретних бінарних симетричних каналів без пам'яті, наприклад, двійкового

симетричного каналу або двійкового каналу зі стиранням. Полярні коди також можуть застосовуватися на недвійкових або безперервних каналах і є оптимальними кодами для стиснення даних з втратами.

Додатковими технологіями в мережах 5G є:

• Massive MIMO - передача до одного абоненту до 8 потоків даних. У Massive MIMO абонент може працювати з великою кількістю антен одночасно, які будуть формувати дуже гострі діаграми спрямованості. Використання просторового мультиплексування декількох променів дозволить збільшити приймаємий рівень сигналу і придушити інтерференцію від інших користувачів, тим самим збільшити пропускну здатність і спектральну ефективність;

Зважаючи на малі довжин хвиль в міліметровому діапазоні, в системах 5G можуть бути використані менші за розмірами антенні системи. Зокрема, особливий інтерес і зусилля на сьогодні прикуті до технологій багатоелементних MIMO антен (Massive-MIMO). Застосування таких антенних технологій дозволяє ефективно вирішувати проблеми повнонаправленного радіозв'язку та інтерференції. З іншого боку, необхідність роботи в таких високих діапазонах спричиняє подорожчання і ускладнення конкретних схемотехнічних рішень.

• Novel Multiple Access - нові технології доступу, наприклад, SCMA;

• New Full Duplex - дозволяє застосовувати одну частоту в різних сотах для різних завдань (UpLink і DownLink);

• Flexibel Duplex - дозволяє організувати гнучку передачу трафіку. Тобто, наприклад, в UPLink передавати інформацію для DownLink;

• FBMC / UFMC (Filter Bank Multicarrier, Universal Filter Multi-Carrier) - збільшує спектральну ефективність, покращує канальну селективність, дозволяє використання в "когнітивному радіо";

• Adv. Coding and Modulation - застосування сукупності технологій модуляцій і кодування, серед яких такі як Non-binary coding, Bit-mapping techniques, Joint coding & modulation;

• Ultra-dense networking - дозволяє за рахунок віртуалізації організувати занадто щільні мережі, за рахунок яких на n-ій площі можна буде обслуговувати велику кількість абонентів, що в свою чергу дозволяє будувати складні ієрархії мережі. Також дана технологія дозволяє одночасну взаємодію сот між собою.

• Low latency & high reliability - зниження затримки і підвищення надійності;

• M2M / D2D - передача інформації безпосередньо між пристроями (машинами, девайсами) без участі людини. Розширення покриття за рахунок пристроїв абонентів Побудова децентралізованої мережі;

• High frequency communication - частоти нижче 6 ГГц будуть первинними діапазонами для мережі 5G. Частоти вище 6ГГц для універсального доступу і

магістрального зв'язку. Як видно з малюнка нижче, планується задіяти частотний діапазон аж до 100 ГГц;

• Spectrum sharing - спільне використання спектра на різних рівнях різними технологіями доступу.

Алфімов Володимир Володимирович
Держаний університет телекомунікацій
факультет Телекомунікацій
м. Київ

ПЕРСПЕКТИВА ВПРОВАДЖЕННЯ ІОЕ В УКРАЇНІ. НАЯВНІ ПРОЕКТИ

У доповіді розкрито поняття «Інтернет усього» та перспективу впровадження його в Україні на прикладі міста Києва. «Internet of Everything» - це нещодавній термін, що означає мережу пристроїв, які відстежують стан інфраструктури квартири/району/міста/країни та обладнання, що аналізує отримані дані та приймає на основі їх контрольні рішення. В місті Києві в останній час впроваджується проект "Smart City", який дозволяє приблизити місто Київ до міста європейського рівня та оптимізувати роботу міських служб.

На даний час Інтернет пройшов чотири етапи розвитку:

-перший етап почався більше 20 років тому та отримав назву «зв'язок». Електронна пошта, просмотр веб-сторінок та пошук контенту тільки починали розвиватись;

-другий етап почався у кінці 90-х років. Він носить назву «сітьової економіки». Час зародження електронної комерції та перетворення ланцюгів постачання у цифровий вигляд. Ми почали покупати іншим шляхом, а компанії завойовували нові ринки;

-третій етап почався у початку 2000-х років; він знайомий як етап «співпраці». На цьому етапі стали популярні соціальні мережі, мобільний зв'язок, відео та облачні обчислення;

-цій етап називається «Інтернетом усього». Даний етап об'єднує людей, процеси, дані та речі, перетворюючи інформацію у дії, які створюють нові можливості.

Останній етап розвитку характеризується активним впровадженням Інтернету у міські служби. Гарний приклад – місто Барселона. У цьому європейському місті, численністю майже 2 млн. людей, майже не буває автомобільних заторів. А все тому, що діє спеціальна система актуалізації заторів та відслідковування парко місць та міського дорожнього трафіку. Таким чином, якщо, наприклад ви виїхали з дому о 8 30 ранку і вам треба бути на роботі о 9, вам треба лише зайти у мобільний додаток, ввести початкову та кінцеву точки маршруту, та програма запропонує вам найкоротший маршрут. Після того, як ви будете неподалік парковки, додаток визначить вільні місця поруч.

Це все досягається системою, яка діє за допомогою Інтернету. Усі камери спостереження підключені до контролеру, який зчитує зображення, та датчики, які визначають густину руху. Таким чином на контролері формується значний обсяг даних. Далі ці дані поступають на сервер, який за допомогою певної служби чи служб, видає результат у вигляді вільних місць та заторів. Крім цього, окрема служба контролює включення та відключення світлофорів. Наприклад, якщо це година-пік, то світлофори включають зелене світло десь раз у 5-7 хвилин, дозволяючи значній частині жителів міста добратись додому вчасно та розвантажити рух.

Майже така ж сама ситуація в Кракові, польському місті. Звісно, там не настільки продумана система вирішення заторів, але ж найкоротший маршрут ви зможете знайти, якщо на зупинці ви відкриєте інтерактивну карту Google та просто введете дві точки – кінцеву та початкову.

Весь цей проект оснований на використанні Інтернету. Схема представляє собою пристрої зчитування даних, контролер, який направляє дані, та механізм обробки у вигляді серверів. У цьому проекті поєднано два типи взаємодії – M2M, P2M, тобто машина-з-машиною та людина-з-машиною. В рамках цієї взаємодії заснований проект «Київ Smart City». Пропонується впровадження такої ж системи відслідковування в місті Києві.

Крім цього, враховуючи особливості культури та інфраструктури міста, та теперішній стан економіки, пропонується також зробити сервіси та послуги, основані на використанні Інтернету. Деякі зміни вже впроваджені чи на стадії впровадження:

-онлайн бюджет – для забезпечення прозорості та доступу до інформації про стан планування та використання бюджетних коштів;

-електронні закупівлі – контроль прозорого та ефективного витрачання бюджетних коштів, державних закупівель, комерційних майданчиків;

-система управління майном – система управління комплексом КМДА для запровадження ефективних засобів використання, контролю та виконання прийнятих рішень щодо майнових ресурсів міста;

-єдина система обліку – інформаційна система управління КМДА з оптимізацією бізнес процесів, утворення тарифів;

- електронні послуги для надання адміністративних та публічних послуг жителям міста.

- триває впровадження системи «Електронний паспортний стіл», яка дозволяє перенести всю базу жителів у електронний вигляд та працювати значно простіше з нею.

Таким чином, перехід інфраструктури міста до електронного управління та «Інтернету усього» значно спрощує життя людей, економить кошти та дозволяє досягти реально європейського рівня обслуговування. Перехід до електронної системи триває, однак слід зазначити, що маленькі зміни вже принесли значні результати в державному управлінні.

Список використаних джерел:

1. Cisco, Internet of everything - http://ioeassessment.cisco.com/
2. Kyiv,Smart city - http://kscf.in.ua/Smart_City_UKR_Print_final.pdf

Бердник Ірина Ігорівна
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

ВЛАСТИВОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Роль і значення ІТ для сучасного етапу розвитку суспільства є стратегічно важливими, і їх значення для економіки країн в цілому буде швидко зростати. Підтвердженням цього є ряд унікальних властивостей ІТ:

• вони дозволяють активізувати й ефективно використовувати інформаційні ресурси як підприємства, так і суспільства в цілому. Активізація, поширення та ефективне використання ІР підприємств дозволяють одержати істотну економію інших видів ресурсів - сировини, енергії, корисних копалин, матеріалів і устаткування, людських ресурсів;

• сприяють оптимізації та автоматизації діяльності співробітників підприємств і членів суспільства, в якому об'єктами і результатами праці більшості зайнятого населення стають уже не матеріальні цінності, а інформація і наукові знання;

• виступають важливими елементами інших більш складних виробничих чи соціальних явищ, тому є дуже важливими компонентами відповідних виробничих чи соціальних технологій.

Інформаційні технології сьогодні відіграють винятково важливу роль і в забезпеченні інформаційної взаємодії між людьми. Вони швидко асимілюються з культурою суспільства, так як створюють великі зручності, знімають багато виробничі, соціальні та побутові проблеми, які викликаються процесами глобалізації та інтеграції світової спільноти, розширенням внутрішніх і міжнародних економічних і культурних зв'язків, міграцією населення.

В якості основних властивостей ІТ, які роблять її здатною до включення в систему управління яким-небудь об'єктом, можна виділити:

• документовані - можливість її подання на матеріальних носіях відповідно до діючих правил оформлення документації;

• надійність - характеризує реалізації в процесі експлуатації всіх її функцій у відповідності з заданими вимогами;

• завершеність - ймовірність виявлення помилок, допущених при її розробці;

• зрозумілість і ясність - відома простота в освоєнні користувачем;

• відкритість і розширюваність - властивість ІТ, що характеризується можливістю введення в неї нових елементів і зв'язків;

• ресурсомісткість - властивість, що характеризується обсягом ресурсів, необхідних для її реалізації;

• формализованность - можливість приведення ІТ до абстрактного увазі;

• захищеність - здатність фіксувати або блокувати дії з несанкціонованого доступу до інформації або спроби її руйнування;

• ефективність - властивість, що характеризується сукупністю ефективностей технічного, економічного і соціального характеру при її використанні.

Класифікація інформаційних технологій

Розглянемо ще одне визначення технології як представлене в проектній формі, концентроване вираження наукових знань і практичного досвіду, що дозволяє раціональним чином організувати будь-який процес з метою економії витрат праці, енергії матеріальних ресурсів або ж соціального часу, необхідних для реалізації цього процесу.

Доцільно виділити три основні класи технологій:

1) виробничі - спрямовані на оптимізацію процесів у сфері матеріального виробництва товарів і послуг та їх суспільного розподілу;

2) інформаційні - призначені для раціональної організації процесів, що протікають в інформаційній сфері суспільства, включаючи науку, культуру, освіту, засоби масової інформації та інформаційні комунікації;

3) соціальні - орієнтовані на раціональну організацію соціальних процесів.

Інформаційні процеси широко використовуються в різних сферах діяльності сучасного суспільства. Вони часто є компонентами інших, більш складних процесів - управління, виробництва, соціальних процесів. Для організації цих процесів використовуються і відповідні їм технології - виробничі чи соціальні, тому й інформаційні технології можуть бути компонентами цих більш складних технологій.

Головна особливість ІТ полягає в їх цільової спрямованості на оптимізацію інформаційних процесів, тобто процесів, вихідним результатом яких є інформація. В якості загального критерію ефективності ІТ будемо використовувати економію соціального часу, необхідного для реалізації інформаційного процесу, організованого відповідно до вимог та рекомендацій цієї технології.

Література:

1. http://pidruchniki.com/11821006/informatika/vlastivosti_informatsiynoyi_tehnologiyi_vimogi_neyi
2. http://stud.com.ua/35746/informatika/vlastivosti_informatsiynih_tehnologiy
3. http://ukrbukva.net/58510-Svoiystva-i-klassifikaciya-informacionnyh-tehnologiiy.html

Скаба Світлана Миколаївна
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Під інформаційними технологіями слід розуміти комплекс взаємозалежних, наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і зберіганням інформації; обчислювальну техніку і методи організації і взаємодії з людьми і виробничим устаткуванням, їх практичні додатки, а також зв'язані з усім цим соціальні, економічні та культурні проблеми.

Сучасна інформаційна технологія орієнтована на застосування найширшого спектру технічних засобів електронно-обчислювальних машин і засобів комунікацій. На її основі створено та створюються обчислювальні системи й мережі різних конфігурацій не тільки для нагромадження, зберігання, перероблення інформації, але й максимального зближення термінальних улаштувань до робочого місця спеціаліста та для підтримки прийняття рішення керівника.

Одна з сучасних тенденцій розвитку інформаційних технологій — напрям технології «клієнт—сервер». Цей підхід реалізується в технології зв’язування та запровадження об’єктів (OLE), організації локальних мереж і мережевих операційних систем, у глобальних мережах типу Internet, в архітектурі систем керування базами даних, в архітектурі пакетів прикладних програм.

Зараз настала ера глобального взаємопов’язаного суспільства, в якому фірми можуть використовувати комп’ютерні інформаційні технології, щоб працювати зі своїми діловими партнерами та клієнтами в світовому масштабі. Інформація стає ресурсом нарівні з матеріалами, енергією і капіталом. Вона перетворюється в один з найбільш цінних за змістом і масових за формою продуктів цивілізації, споживачем якої стає все людство. Машинна інтуїція (експертні системи) перетворюється на продуктивну силу, а штучний інтелект дозволяє вирішувати якісно нові завдання технічного прогресу.

Особливої уваги заслуговує опис унікальних можливостей засобів нових інформаційних технологій, реалізація яких створює передумови для небувалої в історії педагогіки інтенсифікації освітнього процесу, а також створення методик, орієнтованих на розвиток особистості учня-студента, такі як:

1.Негайний зворотний зв’язок між користувачем і засобами нових інформаційних технологій;

2.Комп’ютерна візуалізація навчальної інформації про об’єкти чи закономірності процесів, явищ, як таких, що реально відбуваються, так і «віртуальних»;

3.Архівне зберігання досить великих обсягів інформації з можливістю її передачі, а також легкого доступу та звернення користувача до центрального банку даних;

4.Автоматизація процесів обчислювальної інформаційно-пошукової діяльності, а також обробки результатів навчального експерименту з можливістю багаторазового повторення фрагмента чи самого експерименту;
5.Автоматизація процесів інформаційно-методичного забезпечення, організаційного управління навчальною діяльністю та контролю за результатами засвоєння.

Реалізація перерахованих вище можливостей засобів нових інформаційних технологій дозволяє організувати такі види діяльності як:
1.Реєстрація, збір, накопичення, зберігання, обробка інформації про досліджувані об'єкти, явища, процеси, в тому числі такі які реально протікають, і передача досить великих обсягів інформації, представленої в різних формах;
2.Інтерактивний діалог – взаємодія користувача з програмною (програмно-апаратною) системою, що характеризується на відміну від діалогового, який передбачає обмін текстовими командами (запитами) і відповідями (запрошеннями), реалізацією більш розвинених засобів ведення діалогу (наприклад, можливість задавати питання в довільній формі, з використанням «ключового» слова, у формі з обмеженим набором символів); при цьому забезпечується можливість вибору варіантів змісту навчального матеріалу, режиму роботи;
3.Управління реальними об'єктами (наприклад, навчальними роботами, що імітують промислові пристрої або механізми);
4.Управління відображенням на екрані моделей різних об'єктів, явищ, процесів, в тому числі і таких що реально протікають;
5.Автоматизований контроль (самоконтроль) результатів навчальної діяльності, корекція за результатами контролю, тренування, тестування.

Варто розглянути вплив інформаційних технологій на розвиток соціальних мереж, які є дієвим засобом і особливим інструментом маркетингу.

Соціальна мережа – це структура, що базується на соціальних зв'язках та взаємних інтересах окремих індивідів та організацій в цілому. Завдання такого ресурсу полягає в забезпеченні користувачів усіма можливим засобами взаємодії одне з одним – відео, чатами, зображеннями, музикою, блогами тощо.

За кілька останніх років соціальні мережі стали найпопулярнішими ресурсами в Інтернеті: сьогодні Facebook, Twitter і Linkedin у США й Західній Європі, а Вконтакте й Однокласники в країнах СНД – це сайти з мільйонами активних користувачів. Ці ресурси відвідують 75% українських користувачів Інтернету.

Сучасне суспільство наповнене і пронизане потоками інформації, які потребують обробки. Тому без інформаційних технологій, так само як без енергетичних, транспортних і хімічних технологій, воно нормально функціонувати не може.

Література:

1. http://pidruchniki.com/15290527/informatika/suchasni_informatsiyni_tehnologiyi_programno-tehnologichniy_kompleks_smart_board

2. http://it-tehnolog.com/statti/novi-informatsiyni-tehnologiyi-v-osviti
3. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=juu_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=PREF=&S21COLORTERMS=0&S21STR=Sitimn

Кравцова Майя Олегівна
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

СУЧАСНИЙ РОЗВИТОК ІТ-ТЕХНОЛОГІЙ

Розвиток ІТ-технологій допомагає підвищити ефективність суспільного виробництва в усіх сферах. Можливість пошуку, управління, обробки та обміну інформацією розкриває нові горизонти, дозволяє максимально автоматизувати будь-які виробничі процеси, підвищити показники праці і спростити управління бізнесом.

Основні риси сучасних ІТ:

- структурованість стандартів цифрового обміну даними алгоритмів;
- широке використання комп'ютерного збереження і надання інформації в необхідному вигляді;
- передача інформації за допомогою цифрових технологій на практично безмежні відстані.

За типом оброблюваної інформації ІТ-технології можна умовно розділити на такі види:

- дані (алгоритмічні мови, табличні процесори);
- текст (текстові процесори і гіпертекст);
- графіка (графічні процесори);
- знання (експертні системи);
- об'єкти реального світу (мультимедіа).

Сучасні інформаційні технології також можна класифікувати за типами користувальницького інтерфейсу. Прикладний інтерфейс дозволяє реалізувати функціональні ІТ, а системний містить в собі набір прийомів для взаємодії з комп'ютером. Цей набір може реалізуватися операційною системою або її надбудовами.

До інформаційних технологій пред'являються вимоги:

- диференціація - можливість розбивати весь процес на окремі фази, етапи та дії;
- повнота - наявність всього необхідного набору інструментів;
- регулярний характер - стандартизація та уніфікація всіх етапів для максимально ефективного управління інформаційними процесами.

Забезпечуючі інформаційні технології (ЗІТ) - забезпечують вирішення конкретних завдань різного рівня складності шляхом застосування певних компонентів і програмних засобів.

Функціональні інформаційні технології (ФІТ) є модифікацією забезпечуючих технологій спрямованих на вирішення специфічних завдань. Перехід ВІТ в ФІТ здійснюється шляхом перетворення загальнокорисного інструментарію в спеціальний.

Впровадження ІТ в усі сфери діяльності людини - це процес інформатизації суспільства. Головна мета інформатизації - підвищення ефективності суспільного виробництва в усіх його напрямках. Володіння інформацією, можливість її переробки та обміну, допомагає значно скоротити фінансові втрати, витрати часу і сил на виконання певних операцій.

У сучасному суспільстві інформація стала такою ж необхідною, як освіта, кадри, гроші та інші матеріальні цінності, тому її вільний потік може привести до значного підвищення рівня життя кожної людини.

Для вирішення завдань інформатизації застосовуються інформаційні системи, що реалізують відповідні інформаційні технології.

Інформаційна технологія - це сукупність методів, виробничих процесів і програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збір, обробку, зберігання, передачу і відображення інформації.

Мета функціонування цього ланцюжка, тобто інформаційної технології, - це зниження трудомісткості процесів використання інформаційного ресурсу і підвищення їх надійності та оперативності. Ефективність же інформаційної технології визначається кваліфікацією суб'єктів процесів інформатизації. При цьому технології повинні бути максимально доступні споживачам.

Сучасні інформаційні технології повинні бути максимально доступними споживачам, щоб вони могли без витрат часу і сил проводити різні операції. Організація швидкого доступу до всіх інформаційних ресурсів, необхідних для роботи, гарантує підвищення економічних показників підприємств будь-якого сектору та поліпшення умов праці для персоналу.

Література:

1. http://www.sviaz-expo.ru/ru/articles/sovremennye-informacionnye-tehnologii/
2. http://technologies.su/klassifikaciya_it
3. Wikipedia [Електронний ресурс]

Щетініна Дар'я Артурівна
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ» ім. Сікорського
Факультет Телекомунікацій
м. Київ

ПОНЯТТЯ І ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Технологія як строго наукове поняття означає певний комплекс наукових і інженерних знань, втілений у способах, прийомах праці, наборах виробничо-речових чинників виробництва.

Сучасні інформаційні технології (НІТ) - сукупність методів і засобів одержання і використання інформації на базі обчислювальної та інформаційної техніки, з широким застосуванням інформаційних методів.

У сучасних інформаційних технологіях виділяють 3 складові: апаратне забезпечення (засоби обчислювальної техніки та оргтехніки - hardware); програмне забезпечення (прикладне та системне програмне забезпечення, методичне та інформаційне забезпечення - software); організаційне забезпечення (включаючи людину в системи інформаційних технологій, взаємодія людини з цими системами, системне використання технічних і програмних засобів - orgware).

Як вже говорилося, інформаційні технології застосовуються практично всюди. Технології планування та управління, наукових досліджень і розробок, експериментів, проектування, грошово-касових операцій, криміналістики, медицини, освіти тощо - сьогодні не обходяться без участі комп'ютерів.

Як виробничі, так і інформаційні технології виникають не спонтанно, а в результаті технологізації того або іншого соціального процесу, тобто цілеспрямованого активного впливу людини на ту чи іншу область виробництва і перетворення її на базі машинної техніки. Чим ширше використання ЕОМ, тим вище їх інтелектуальний рівень, тим більше виникає видів інформаційних технологій, до яких відносяться:

- технології планування та управління;
- наукових досліджень і розробок;
- експериментів; проектування;
- грошово-касових операцій;
- криміналістики;
- медицини;
- освіти та ін

Інформаційної технології властиві наступні властивості:

- високий ступінь розчленованості процесу на стадії, що відкриває нові можливості для його раціоналізації і перекладу на виконання за допомогою машин, Це - найважливіша характеристика машинізованого технологічного процесу;
- системна повнота (цілісність) процесу, який повинен включати весь набір елементів, що забезпечують необхідну завершеність дій людини при досягненні поставленої мети;
- регулярність процесу й однозначність його фаз, що дозволяють застосовувати середні величини при їхній характеристиці, і, отже, допускають їх стандартизацію та уніфікацію. В результаті

з'являється можливість обліку, планування, диспетчеризації інформаційних процесів.

У такій розвинутій формі, що має всі ознаки відмічені, інформаційно-комунікативні процеси присутні в машинізоване кібернетичних системах. Інформатика вивчає загальні моменти, властиві всім численним різновидам конкретних інформаційних технологій.

Література:

1. http://www.infuha.ru/news/read/informacijni_tehnologii_ta_iz_vudu.html
2. http://ukrarticles.pp.ua/pk-internet/6918-znachenie-informacionnyx-texnologij-v-sovremennom-obshhestve.html

Аношко Микита Ігорович
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

«ВЕЗДЕ НА СВЯЗИ»: ИНТЕРНЕТ НА ВОДЕ, В ВОЗДУХЕ И КОСМОСЕ

Мы привыкли к тому, что имеем постоянный доступ к Сети. Но как обстоят дела с доставкой связи в «труднодоступные» места? Об этом мы и поговорим сегодня.

Вода

Интернет в море — это не то же самое, что интернет на материке. Однако он там есть. Наиболее популярный способ доставки интернета на корабли — спутниковая связь. Прямое соединение осуществляется с помощью специализированного аппаратного обеспечения, установленного на судне. Например, несколько лет назад компания «Билайн» настроила спутниковую систему на теплоходе. Была установлена односторонняя тарелка со стабилизаторами и поворотными механизмами, чтобы нивелировать воздействие качки и отслеживать спутник во время движения судна. Для организации исходящего канала использовали ряд 3G-модемов. Ключевой элемент комплекса — однонаправленная антенна Tracvision M9. DVB-поток с антенны поступает на карту DVB-S2 PCI, установленную в обычный персональный компьютер. Балансировщик нагрузки был построен на базе VMware ESXi, внутри которого были развернуты две виртуальные машины: балансировщик на Vyatta и кэш-сервер на Debian. После этого по теплоходу был растянут кабель 5e для подключения беспроводных точек доступа с питанием от коммутаторов Cisco, покрывших почти все рабочие зоны судна.

Космос

Космос имеет свои неоспоримые преимущества. Но скоростной интернет — не одно из них. По словам космонавта Скотта Келли (Scott Kelly), «интернет на МКС гораздо хуже, чем был Dial-Up». Интернет в космосе базируется на сети для отслеживания спутников — этими же средствами коммуникации инженеры НАСА пользуются для общения с космонавтами. НАСА Deep Space Network (DSN) — это интернациональная сеть из антенн, которая обеспечивает связь между инженерами и учеными на Земле и миссиями в космосе. DSN состоит из трех комплексов, «раскиданных» по всей планете: в пустыне Мохаве, США, недалеко от Мадрида, Испания, и недалеко от Канберры, Австралия. Такое расположение позволяет не выпускать МКС из зоны видимости.

DNS-антенны очень большие, и их размеры достигают 70 метров. Чем больше антенна, тем сильнее сигнал, и тем большее количество информации она способна передавать. Обычно самые крупные ретрансляторы DSN задействуются только при чрезвычайных ситуациях. Для большинства космических аппаратов достаточно использования меньших (более экономичных) антенн, как это было во время полета Марсианской научной лаборатории.

Низкая скорость интернета в первую очередь связана с расстоянием, которое приходится преодолевать данным. Когда космонавт кликает на ссылку, запрос пролетает примерно 35 тыс. км от Земли до сети геосинхронных спутников. После этого спутники отправляют ответ вниз на приемник, обрабатывающий его перед трансляцией на МКС.

«Космонавты подключаются не к интернету — они подключаются к компьютеру, который подключен к интернету, — рассказывает Роберт Фрост (Robert Frost), занимающийся подготовкой космонавтов для миссий на МКС. — Зеркалирование выполнено в целях безопасности. Это позволяет экипажу просматривать контент, не рискуя заполучить вредоносное ПО на борт станции».

В связи с этим наблюдаются определенные задержки при обращении к сайтам. «Но не все так плохо, — отмечает Дэн Хуот (Dan Huot), представитель НАСА. – У нас есть возможность передавать в обе стороны «тяжелые» видеофайлы. Каждый день мы передаем туда-сюда гигабайты видеозаписей с камер наблюдения, и это не вызывает серьезной нагрузки на систему». В свободное время команда даже может смотреть телевизионные шоу или фильмы.

Инженеры постоянно работают над улучшением качества соединения. В этом году НАСА также сделало шаг в сторону создания SSI — Solar System Internet, установив сервис DTN — Delay/Disruption Tolerant Networking на МКС. Решение должно автоматизировать и повысить доступность данных для космических экспериментов и привести к более оптимальному использованию пропускного канала.

В сети DTN данные от приложений представляются в виде сообщений произвольной длины и преобразуются в специальные пакеты для пересылки в гетерогенных сетях. Каждая такая посылка состоит из блоков, содержащих как данные приложений, так и команды для доставки. Здесь, как и в IP-сетях, используется принцип «сохрани и передай», предполагающий сохранение пакетов при невозможности их передачи. Только в случае DTN время хранения гораздо больше, поскольку существует высокая вероятность, что канал в момент передачи может оказаться недоступен. На борту МКС функциональность DTN была добавлена в Telescience Resource Kit (TReK) — программный исследовательский комплекс для передачи данных между операционными центрами. Это должно повысить качество работы важных для миссии приложений.

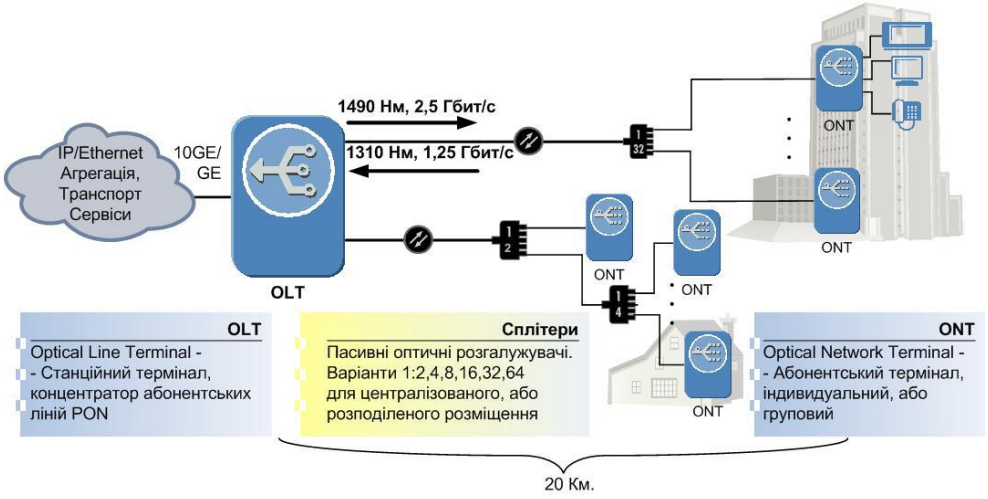
Первое применение сервиса подтолкнуло мир к созданию интернета, работающего в пределах солнечной системы, в котором МКС будет играть важную роль. Более того, в будущем DTN позволит обращаться и в те зоны на планете, где обычные средства коммуникации оказываются недоступны, например, из-за чрезвычайных ситуаций.

ИСТОЧНИК: https://habrahabr.ru/company/vasexperts/blog/315006/

Заруцький Роман Валентинович
Державний Університет Телекомунікацій
Факультет Інформаційних технологій
м. Київ

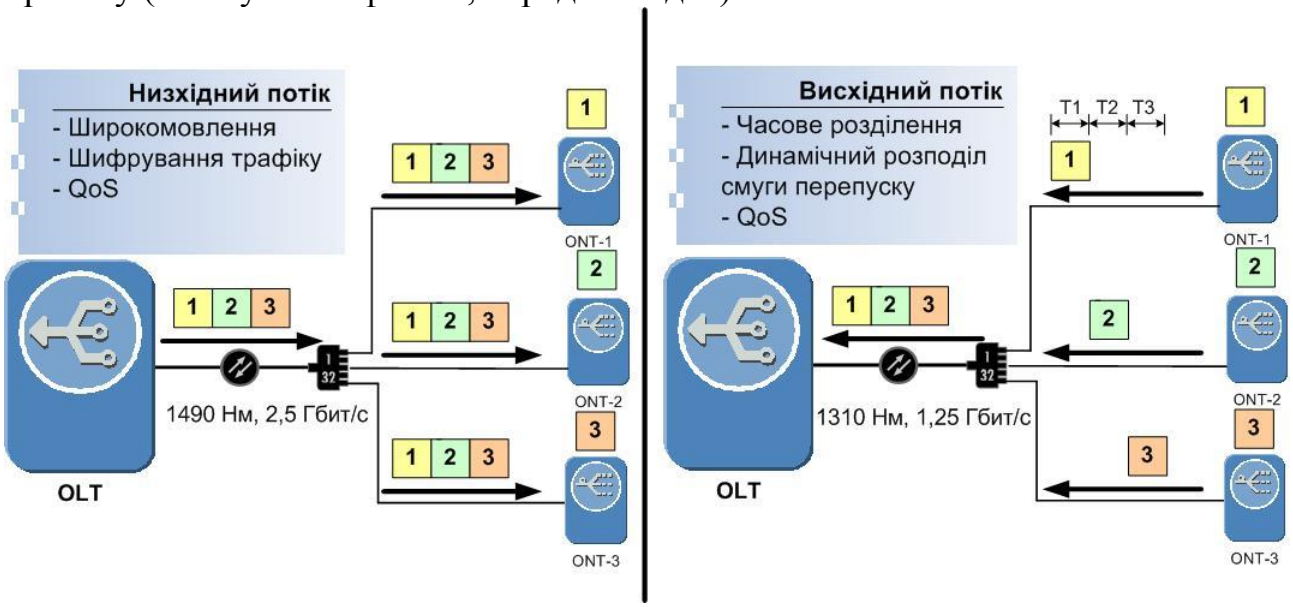
GPON

Технологія GPON входить до сімейства технологій пасивних оптичних мереж доступу PON. Технологію специфіковано у рекомендації ITU-T G.984. Серед інших технологій PON можна виділити застарілі: APON, BPON, EPON; та конкуруючу GEPON. GEPON є стандартом IEEE, та здебільшого присутня на азійських ринках, у глобальному вимірі перевагу надано GPON. Серед переваг GPON можна відзначити найбільшу швидкість, синхронний формат кадру, інтеграцію з ATM та TDM технологіями та визначені плани розвитку.



- Станційного терміналу OLT (англ. *Optical Line Terminal*), який містить у собі певну кількість портів GPON (типово від 4 до 112) та порти Gigabit Ethernet або 10 Gigabit Ethernet для підключення до транспортної IP мережі.
- Абонентського терміналу ONT (Optical Network Terminal). ONT може бути розрахованим на одного користувача та мати порти Ethernet, POTS та RF TV, або на групу користувачів, або на організацію, та мати порти Ethernet, xDSL, POTS, E1, RF TV.
- Повністю пасивної оптичної розподільчої мережі між ними, яка складається зі сплітерів з коефіцієнтом розділення від 1:2 до 1:64, що розташовані централізовано, або розподілено.

Передача з OLT ведеться на довжині хвилі 1490 нм зі швидкістю 2,5 Гбіт/с, а прийом — на довжині хвилі 1310 нм зі швидкістю 1,25 Гбіт/с. Таким чином забезпечується робота системи по одному волокну за принципом WDM. Асиметричність швидкостей потоку обумовлена характером трафіку низхідного протоку (закачування файлів, передача відео).



Одночасна робота багатьох абонентів у одному волокні забезпечується:

- У низхідному потоці (від OLT до ONT) за принципом широкомовлення — усі кадри передаються усім абонента у зашифрованому 128-бітним ключем вигляді, і кожен ONT має доступ своїх кадрів.
- У висхідному потоці працює принцип TDM. Кожен з ONT веде передачу тільки у своєму проміжку часу.

Стабільна та гнучка робота досягається завдяки повній синхронізації мережі разом з динамічним розподілом смуги перепуску.

Побудова розподільної мережі GPON є цікавим і творчим процесом, при якому необхідно враховувати як технічні характеристики, так і економічні аспекти різних топологій. У міській місцевості раціональним є застосування сплітерів малої ємності (1:2 — 1:4 у зовнішній мережі), далі у будинку коефіцієнт сплітера залежить від кількості абонентів (1:8, 1:16, 1:24, 1:32, 1:64) і далі індивідуальне волокно іде до кожного з абонентів. У сільській місцевості

переваги GPON проявляються навіть у більшій мірі. Тут раціональним є встановлення кінцевого сплітера в залежності від групи близьких один до одного домів. Також, окрім FTTH, GPON може використовуватися у FTTB та FTTC топологіях із застосуванням групових ONT.

- Завдяки найвищим швидкостям та механізмам керування трафіком технологія GPON дозволяє надати найкращий та найякісніший пакет послуг та максимізувати прибутки оператора.
- Оптимізація капітальних витрат досягається завдяки концентрації великої кількості абонентів на одне волокно та централізацією та малою кількістю активного обладнання.
- Експлуатаційні витрати є головною статтею економії завдяки GPON. Головні фактори — централізація обладнання та керування мережею, проста та надійна пасивна інфраструктура мережі, відсутність активного обладнання всередині мережі, відповідно значна економія електроенергії та орендних витрат.

Що дає технологія GPON користувачеві?

- **Високошвидкісний Інтернет** на швидкості до 1 Гб/с.
- **Новітнє інтерактивне IP-телебачення**, яке дозволяє не тільки дивитися більше 60 супутникових і ефірних каналів цифрового телебачення, в тому числі 10 каналів з високою роздільною здатністю формату HDTV, але і користуватися інтерактивними сервісами: замовити запис фільму і переглянути його після ефірного показу, переглянути телепередачу, трансляція якої вже відбулася, замовити фільм з відеотеки.
- **Якісний зв'язок** з можливістю підключення як звичайного, так і IP-телефону з розширеним набором функцій, необмежену кількість номерів по одній лінії і збереження номера при переїзді. Використовуючи послуги IP-телефонії можна значно економити на дзвінках в інші міста.

Основні технології GPON

- Принципи GPON - мультиплексування даних. GPON використовує Wavelength Division Multiplexing (WDM) технологію, для забезпечення 2-х спрямованої роботи в 1 оптичному кабелі.

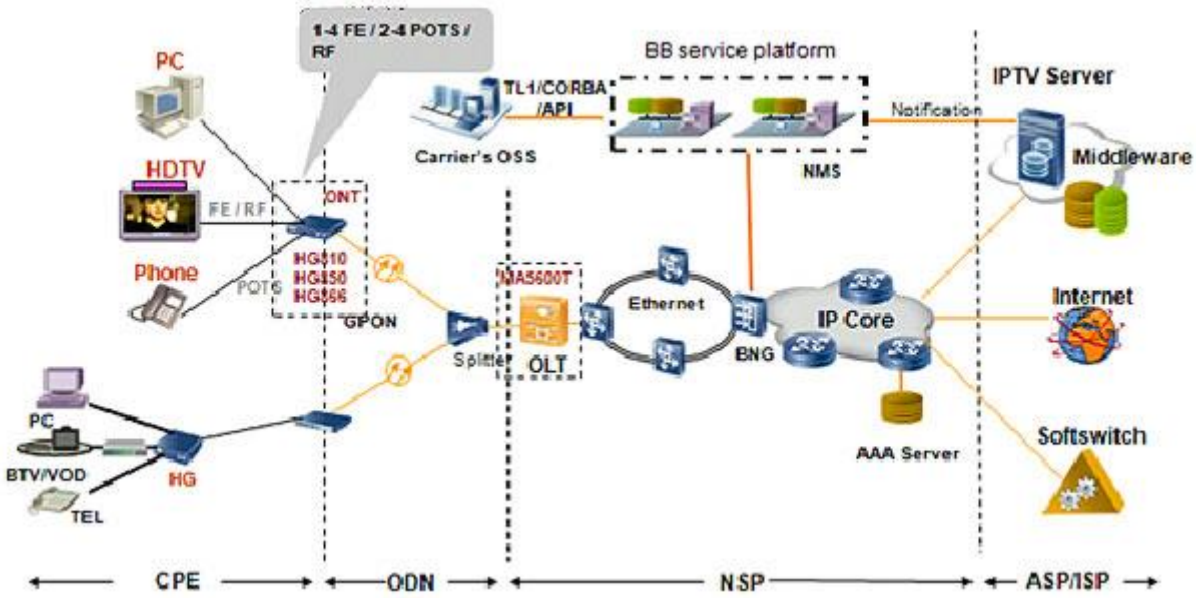
  Для поділу upstream/downstream сигналів для багатьох користувачів через одне волокно, GPON застосовує 2 механізми:

  • У напрямку downstream (довжина хвилі 1490 нм і 1550 нм) пакети даних передаються в режимі broadcast;

  • У напрямку upstream (довжина хвилі 1310 нм) пакети даних передаються в режимі подібному TDMA.
- GPON Downlink. Кадр фіксованої довжини 125 мкс. Розподіл трафіку на основі GEM-PORT з функцією контролю (обмеження смуги).
- GPON Uplink. Послідовність і час доставки пакетів від кожного ONU контролюється OLT.
- Різні конфігурації GPON.

- Ослаблення потужності в технології GPON. Наприклад, обладнання Huawei GPON підтримує тип Class B+ з чутливістю -28dB, що дає впевнений прийом на відстані 20 км.

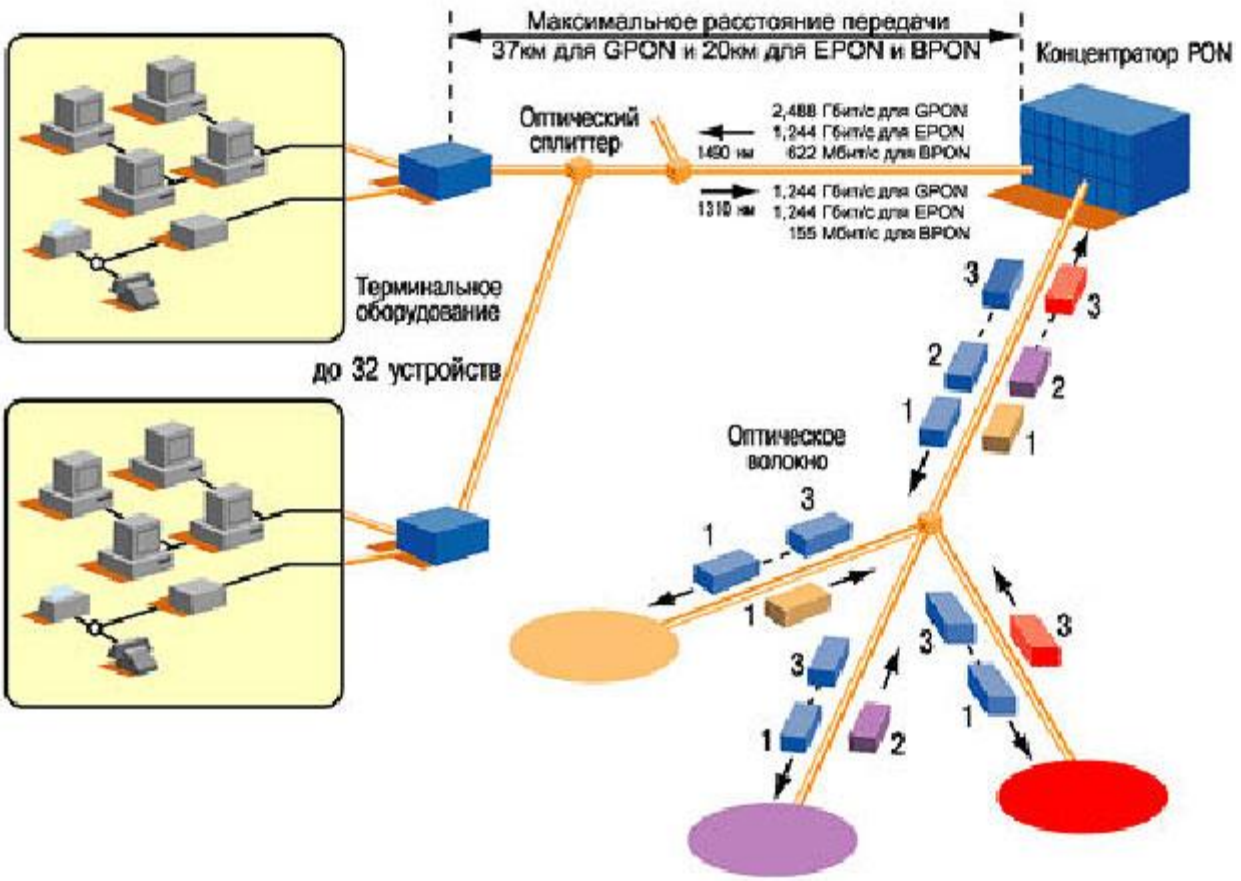
Місце GPON в схемі рішення FTTH для домашніх користувачів:



Центральний вузол PON може мати мережеві інтерфейси ATM, SDH (STM-1), Gigabit Ethernet для підключення до магістральних мереж. Абонентський вузол може надавати сервісні інтерфейси 10/100Base-TX, FXS (2, 4, 8 і 16 портів для підключення аналогових ТА), E1, цифрове відео, ATM (E3, DS3, STM-1c). Більш детально з окремими пристроями, використовуваними в технології, можна ознайомитись в каталозі GPON.

Короткий порівняльний аналіз технологій

	APON	BPON	EPON (GEPON)	GPON
Стандарт	G.983	ITU G.983	IEEE 802.3ah	ITU G.984.6
Полоса пропускання для низхідного потоку	155 Мбіт/с	622 Мбіт/с	1,244 Гбит/с	2,488 Гбіт/с
Полоса пропускання для висхідного потоку	155 Мбіт/с	155 Мбіт/с	1,244 Гбіт/с	1,244 Гбит/с
Ємність, абонентів		32	32	128
Максимальна відстань передавання, км		20	20	60
Затухання в лінії PON			26 дБ	22 дБ

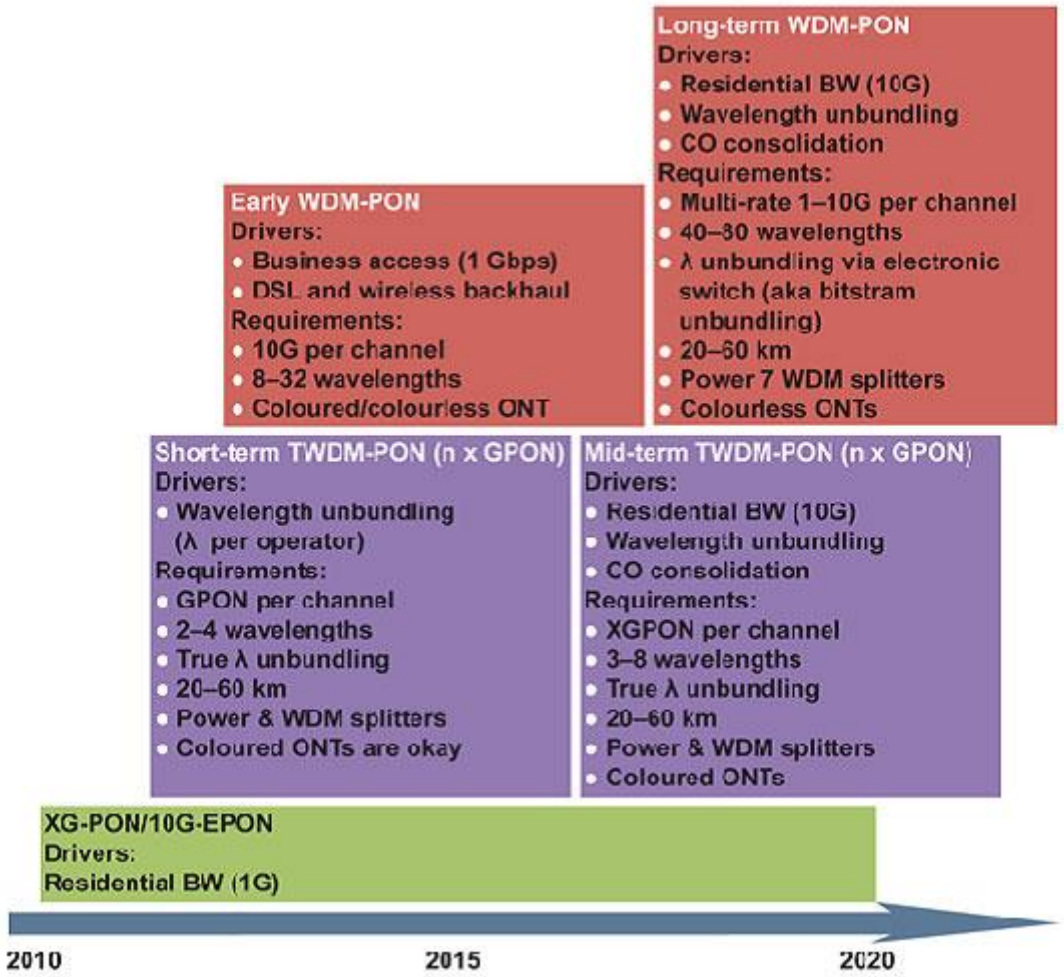


Основні переваги технології PON

- Економія волокон. До 128 абонентів на одне волокно, протяжність мережі до 60 км
- Ефективне використання смуги пропускання оптичного волокна
- Швидкість до 2,488 Гбіт/с по низхідному потоку і 1,244 Гбіт/с по висхідному потоку
- Надійність. У проміжних вузлах дерева знаходяться тільки пасивні оптичні розгалужувачі, які не потребують обслуговування.
- Масштабованість. Деревоподібна структура мережі доступу дає можливість підключати нових абонентів самим економічним способом.
- Можливість резервування як всіх, так і окремих абонентів
- Гнучкість. Використання ATM як транспорту дозволяє надавати абонентам саме той рівень сервісу, який їм потрібен.
- Дані мережею передаються у вигляді осередків ATM
- Можливий симетричний і асиметричний режими роботи

Впровадження GPON

Технологія GPON вже сьогодні займає лідируюче місце на ринку широкосмугового доступу, а перспективи технології PON ще більш вражаючі:



В 2011 році компанія ВАТ МГТС почала модернізацію мережі зв'язку м. Москви в частині заміни застарілої мідної інфраструктури мережі, яка використовується МГТС вже майже 130 років, на якісну оптичну мережу GigabitPON.

Основні переваги нової для Москви технології GigabitPON - це швидкість доступу до ресурсів мережі Інтернет - до 200 Мбіт/с, цифрова якість телефонного зв'язку, можливість збереження номера при переїзді в межах м. Москви і легкість підключення/перемикання. Крім того, GigabitPON - необмежений потенціал для впровадження та розвитку нових послуг (відеоспостереження і телеметрія, охоронно-пожежна сигналізація, IP TV та ін.)

В даний час перемикання з міді на оптичну мережу МГТС виконує безкоштовно.

Щоб побачити, у що «виливається» нова технологія кінцевому користувачеві, наводжу цитату з безлімітних тарифних планів GPON для населення м. Омська (Росія):

На сьогодні існує безліч інших прикладів успішної побудови масштабних комерційних проектів на базі GPON. Це дозволяє оцінити потенціал нової технології, яка швидко стає справжнім «мейнстрімом» в галузі.

Гончаров Євгеній Русланович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Сучасне суспільство важко уявити без інформаційних технологій. Кожна людина хоч раз зверталася за допомогою до інформаційних ресурсів. Сучасність характеризується стабільним зростанням обсягу інформаційних потоків. Це відноситься практично до будь-якій сфері діяльності людини. Інформація являє собою один з основних, вирішальних чинників, який визначає розвиток технології і ресурсів в цілому. У зв'язку з цим, дуже важливо розуміння не тільки взаємозв'язок розвитку індустрії інформації, комп'ютеризації, інформаційних технологій з процесом інформатизації, але і визначення рівня і ступеня впливу процесу інформатизації на сферу управління та інтелектуальну діяльність людини.

Дана тема актуальна, тому що інформаційні технології в своєму розвитку постійно еволюціонують, і дуже важливо розуміти вплив цього розвитку на суспільство.

Інформаційні технології розширюють межі можливостей людини.

Інформаційна технологія - це сукупність методів, виробничих процесів і програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збір, обробку, зберігання, передачу і відображення інформації.

Мета функціонування цього ланцюжка, тобто інформаційної технології, - це зниження трудомісткості процесів використання інформаційного ресурсу і підвищення їх надійності та оперативності.

Ефективність інформаційної технології визначається, в кінцевому рахунку, кваліфікацією суб'єктів процесів інформатизації. При цьому технології повинні бути максимально доступні споживачам.

Можна класифікувати інформаційні технології з різних точок зору. Наприклад: Інформаційні технології можна розрізняти по типу оброблюваної інформації.

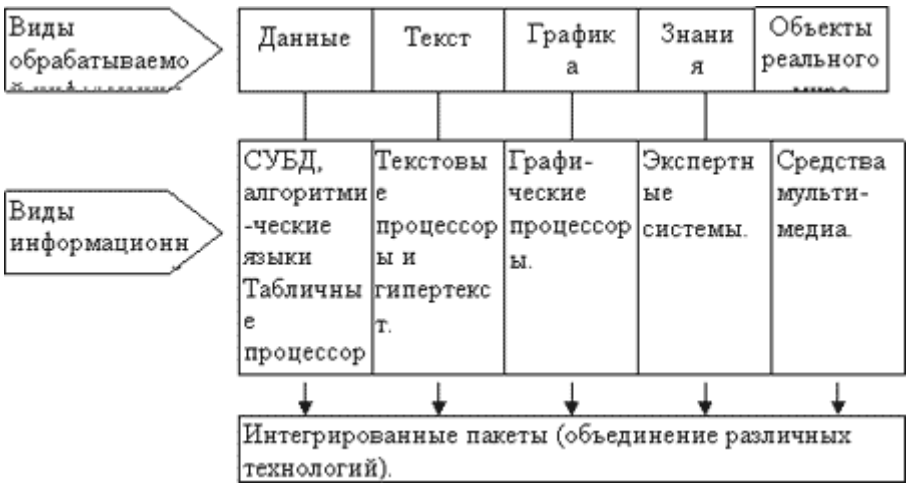


Рис.1. Класифікація ІТ по типу оброблюваної інформації

Поділ досить умовний, тому що більшість інформаційних технологій дозволяє підтримувати і інші види інформації. Наприклад, в текстових процесорах можлива і нескладна розрахункова діяльність, а табличні процесори обробляють не тільки цифрову інформацію, а й можуть генерувати графіки. Однак кожна з видів технології в основному орієнтована на роботу з інформацією певного виду. Модифікація елементів, що становлять інформаційні технології, дає можливість утворення нових технологій в різних комп'ютерних середовищах.

Інформаційні технології можна розділити на забезпечуючі (ЗІТ) і функціональні (ФІТ).

Забезпечуючі технології - це технології обробки інформації, які можуть використовуватися як інструментарій у різних предметних областях. При цьому вони можуть забезпечувати рішення поставити різного плану і різного ступеня складності. ЗІТ можуть бути розділені за класами завдань, в залежності від класу ЗІТ використовують різні види компонентів і програмних засобів.

При об'єднанні ЗІТ по предметній ознаці виникає проблема системної інтеграції, тобто приведення різних технологій до єдиного стандартного інтерфейсу.

Функціональні інформаційні технології (ФІТ) - це модифікація забезпечуючих технологій для задач певної предметної області, тобто реалізується предметна технологія.

Наприклад: робота співробітника технічного відділу великого підприємства.

Ця робота передбачає застосування технологій диспетчерської, бухгалтерії інформаційного відділу і т.д., які в свою чергу реалізовані в своїй інформаційній технології: СУБД, текстові процесори і т.п. Перехід від забезпечуючої інформаційної технології в чистому вигляді в функціональну - це перетворення загальновживаного інструментарію в спеціальний. Таке перетворення стає все більш доступним користувачеві, так як забезпечуючі

технології стають все більш дружніми. Тому в арсеналі працівника технічного відділу зараз можуть бути і його власні забезпечуючі технології (текстові і табличні процесори, наприклад) і спеціальні функціональні технології інших підрозділів (СУБД, диспетчерські та експертні системи), що реалізують предметні технології.

Предметні технології та інформаційна технологія впливають один на одного. Наприклад, поява пластикових карток як носіїв фінансової інформації принципово змінила предметну технологію. При цьому довелося створювати абсолютно нову інформаційну технологію. Але, в свою чергу, можливості, представлені новою ІТ, вплинули на предметну технологію пластикових носіїв (в області їх захисту, наприклад).

Інформаційні технології класифікуються за типами користувальницького інтерфейсу.

Можна виділити системний і прикладний інтерфейс.

Прикладний інтерфейс пов'язаний з реалізацією функціональних інформаційних технологій.

Системний інтерфейс - це набір прийомів взаємодії з комп'ютером, який реалізується операційною системою або її надбудовою. Класифікацію інформаційних технологій за типами призначених для користувача інтерфейсів можна уявити малюнком.

Рис.2. Класифікація ІТ за типами користувальницького інтерфейсу.

Розглянемо докладно класи інформаційних технологій за інтерфейсами.

Командний інтерфейс - забезпечує виведення на екран системного запрошення для введення команди. Наприклад, в MS-DOS це запрошення виглядає так C:>, а в операційній системі UNIX це знак долара $ на екрані.

WIMP - інтерфейс [Winows – Image - Menu - Pointer]. На екрані висвічується вікно, що містить образи програм і меню дії. Для вибору використовується вказівник.

SILK [Speech – Image – Language - Knowledge]. При використанні SILK - інтерфейсу на екрані по мовної команді відбувається переміщення від одних пошукових образів до інших за смисловим зв'язкам.

Сучасні операційні системи підтримують командний SILK інтерфейси. Зараз розробляється так званий суспільний інтерфейс (Social Interface). Громадський інтерфейс, включаючи переваги WIMP і SILK, дозволить, позбавиться від меню, екранні образи вкажуть шлях роботи. Переміщення від одних пошукових образів до інших відбуватиметься по семантичним зв'язкам.

Операційні системи ОС діляться на однопрограмні, багатопрограмні і розраховані на багато користувачів. До однопрограмних відносяться МС-ДОС, до багатопрограмних ОС Windows, DOS 7.0 - вони дозволяють одночасно виконувати кілька додатків. Одно - і багатопрограмні ОС відрізняються алгоритмом поділу часу. Однопрограмні працюють або в пакетному режимі, або в діалоговому. Багатопрограмні поєднують ці режими. Таким чином, ці операційні системи забезпечують пакетну і діалогову інформаційні технології.

Системи, які розраховані на багато користувачів реалізуються мережевими операційними системами. Вони забезпечують віддалені мережеві технології.

Всі три типи інформаційних технологій знаходять найширше застосування в інформаційних системах будь-якої орієнтації - економічних, технологічних і т.д.

Більшість забезпечуючих і функціональних технологій використовуються користувачем без посередників - програмістів. Користувач може самостійно змінювати послідовність застосування тих чи інших технологій. З точки зору участі або неучасті користувача в інформаційному процесі, технології можна розділити на пакетні і діалогові.

Завдання, які вирішуються в пакетному режимі, характеризуються такими властивостями:

алгоритм вирішення задачі формалізований, процес не вимагає втручання людини.

є великий обсяг вхідних і вихідних даних; значна їх частина зберігається на магнітних носіях.

великий час вирішення завдань, обумовлене обсягами даних.

регламентность, тобто завдання вирішуються із заданою періодичністю.

Діалоговий режим - це не альтернатива пакетного режиму, а його розвиток. Діалоговий режим дозволяє користувачеві втрутитися в процес вирішення завдання, він відпускає користувача, скасовує жорстко закріплену послідовність обробки даних. Застосування режимів залежить в першу чергу від предметної технології.

Інтерфейс включає в себе три поняття: спілкування додатком з користувачем, спілкування користувача з додатком, мова спілкування

(визначається розробниками програмного додатка). Властивості призначеного для користувача інтерфейсу: конкретність і наочність. Раніше командний інтерфейс мав багато різноманітних команд, був відсутній стандарт для додатків. Перший вдалий крок для впорядкування роботи в діалогової технології зробив Пітер Нортон, створивши Norton Commander (NC). Наступним вирішальним кроком стало створення графічної оболонки для операційної системи. Зараз практично всі операційні системи використовують графічний інтерфейс. Наприклад, відома всім операційна система Microsoft Windows реалізує технологію WIMP. Нововведенням було застосування миші, вибір команд з меню, надання програмам окремих вікон, використання піктограм для зображення програм.

Зручність інтерфейсу і багатство можливостей роблять Windows оптимальною системою. Програми, написані під Windows, використовують той же інтерфейс, що дозволяє швидко з ними почати працювати без тривалого навчання.

Однією з важливих функцій інтерфейсу є формування у користувача однакових реакцій на однакові дії додатків, узгодженість.

Узгодження слід розглядати з трьох сторін:

з фізичної сторони - з точки зору технічних засобів.

з синтаксичного боку - послідовність і порядок появи елементів на екрані (мова спілкування) і послідовність запитів (мова дій).

з семантичного боку - значення (смислових) елементів, що становлять інтерфейс.

Узгодженість всіх сторін інтерфейсу необхідна і розробнику, і користувачеві. Розробнику узгодженість дозволить виділити загальні блоки, стандартизувати окремі елементи (тим самим скоротити час на їх розробку). Для користувача узгодженість інтерфейсу скорочує час вивчення, число помилок.

Розробка користувальницького інтерфейсу полягає в проектуванні панелей і діалогу. Панель додатка розділена на три частини: меню дій, тіло панелі і область функціональних клавіш.

Меню дій містить об'єкти, що складаються з одного або декількох слів. Розміщуються об'єкти зліва на право у напрямку зниження частоти їх використання. Можливі варіанти з багаторівневою системою "випадаючого меню", хоча реально рівнів не повинно бути більше трьох.

Тіло панелі містить ряд елементів: роздільники областей, ідентифікатор і заголовок панелі; інструкція; заголовок стовпчика, групи, поля; вказівник протягання; області повідомлень і команд; поля введення і вибору.

Область функціональних клавіш: (може й не бути) показує відповідність клавіш і дій, які виконуються при їх натисканні. Вказуються тільки дії, доступні при роботі на поточній панелі.

Коли користувач і ЕОМ обмінюються повідомленнями, діалог рухається по одному з шляхів Додатка. При цьому Додаток може виконувати деякі конкретні дії.

Шлях, по якому рухається діалог, називають навігацією. Навігація може бути зображена у вигляді графа. На графі вузли - дії, дуги - переходи.

Діалоги складається з двох частин:

- запити на обробку інформації;
- навігація по Додатку.

Уніфіковані дії діалогу мають однаковий сенс у всіх додатках. (Наприклад "відмова" "введення" "вихід" "підказка" і т.д.)

Таким чином призначений для користувача інтерфейс є основним фактором в ефективному використанні інформаційних технологій.

Можна класифікувати інформаційні технології за ступенем їх взаємодії між собою. Наприклад, дискретна і мережева взаємодія; взаємодія з використанням різних варіантів обробки і зберігання даних; розподілена інформаційна база і розподілена обробка даних. Цю класифікацію інформаційних технологій можна зобразити за допомогою схеми.

Рис.3. Класифікація ІТ за ступенем взаємодії

Гончаров Євгеній Русланович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Сучасне суспільство важко уявити без інформаційних технологій. Кожна людина хоч раз зверталася за допомогою до інформаційних ресурсів. Сучасність характеризується стабільним зростанням обсягу інформаційних потоків. Це відноситься практично до будь-якій сфері діяльності людини. Інформація являє собою один з основних, вирішальних чинників, який визначає розвиток технології і ресурсів в цілому. У зв'язку з цим, дуже важливо розуміння не тільки взаємозв'язок розвитку індустрії інформації, комп'ютеризації, інформаційних технологій з процесом інформатизації, але і визначення рівня і ступеня впливу процесу інформатизації на сферу управління та інтелектуальну діяльність людини.

Дана тема актуальна, тому що інформаційні технології в своєму розвитку постійно еволюціонують, і дуже важливо розуміти вплив цього розвитку на суспільство.

Інформаційні технології розширюють межі можливостей людини.

Інформаційна технологія - це сукупність методів, виробничих процесів і програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збір, обробку, зберігання, передачу і відображення інформації.

Мета його функціонування - це зниження трудомісткості процесів використання інформаційного ресурсу і підвищення їх надійності та оперативності.

Ефективність інформаційної технології визначається кваліфікацією суб'єктів процесів інформатизації.

Можна класифікувати інформаційні технології з різних точок зору. Наприклад: Інформаційні технології можна розрізняти по типу оброблюваної інформації.

Інформаційні технології можна розділити на забезпечуючі (ЗІТ) і функціональні (ФІТ).

Забезпечуючі технології - це технології обробки інформації, які можуть використовуватися як інструментарій у різних предметних областях.

Функціональні інформаційні технології (ФІТ) - це модифікація забезпечуючих технологій для задач певної предметної області, тобто реалізується предметна технологія.

Інформаційні технології класифікуються за типами користувальницького інтерфейсу.

Можна виділити системний і прикладний інтерфейс.

Прикладний інтерфейс пов'язаний з реалізацією функціональних інформаційних технологій.

Системний інтерфейс - це набір прийомів взаємодії з комп'ютером, який реалізується операційною системою або її надбудовою. Класифікацію інформаційних технологій за типами призначених для користувача інтерфейсів можна уявити малюнком.

Можна класифікувати інформаційні технології за ступенем їх взаємодії між собою. Наприклад, дискретна і мережева взаємодія; взаємодія з використанням різних варіантів обробки і зберігання даних; розподілена інформаційна база і розподілена обробка даних.

Крочак Руслан Петрович
Державний університет телекомунікацій
Телекомунікаційні системи та мережі
Факультет Телекомунікацій
м. Київ

ТЕХНОЛОГІЯ АИС

Суттю этой статьи является объяснить принципы работы автоматической идентификационной системы, особенности её работы, сферы использование и безопасности.

АИС (Автоматическая идентификационная система, (англ. AIS Automatic Identification System) — система в судоходстве, служащая для идентификации судов, их габаритов, курса и других данных с помощью радиоволн диапазона ультракоротких волн. АИС предназначена для отображения информации о надводной обстановке посредством передачи в эфир на частоте 161,975 МГц как статической, так и динамической информации о судне и других объектах,

К динамической информации относится:

Номер морской подвижной службы (MMSI) - уникальный идентификационный номер для каждого судна станции флаг судна может не учитываться)

AIS Навигационный статус - каждый корабль имеющий АИС также сообщает свой статус, то есть чем занимается в данное время. Примеры статусов: 0 = на ходу с использованием двигателя

1 = на якоре

3 = ограниченная маневренность

5 = пришвартован

6 = на мели

7 = занимается рыболовством

8 = в плавании, и другие.

Скорость поворота - вправо или влево (от 0 до 720 градусов в минуту)
UTC секунды - поле секунд времени UTC и прочие.

К статической информации относится:

Международная морская организация номер (IMO) - это число остается неизменным при передаче регистрации субъекта судна в другую страну (флаг)
Позывные - международный радиопозывные назначен на судно ее страной регистрации
Имя - до 20 символов
Тип (или тип груза) - АИС идентификатор shiptype подчиненного судна
Размеры - округляется до ближайшего метра (на основании положения станции АИС на судне)
Расположение антенны системы позиционирования, установленной на борту судна
Тип системы определения местоположения (GPS, DGPS, Loran-C)
Осадка - от 0,1 до 25,5 метров
Пункт назначения - до 20 символов
ETA (приблизительное расчетное время прибытия) - UTC месяц / день часы: минут. С помощью этой технологии возможен обмен данными судов и наземных станций через наземное радиовещание, или через спутниковою связь.

Состав системы АИС

Технически система АИС представляет из себя приемопередающее устройство – АИС-транспондер, антенный кабель с двумя разъемами, УКВ антенну морского диапазона с креплением, и по необходимости дисплей для индикации поступающих сведений. По сути это радиостанция (или радиомодем), ведущая прием и передачу установленных и поступающих данных в автоматическом режиме на установленных частотах с заданным интервалом времени.
Для посыла динамической информации АИС-транспондер должен быть скоммутирован в навигационную информационную сеть судна или иметь возможность совершать самому расчет навигационных задач, для этого он оснащается дополнительно антенной приемника (GPS/ГЛОНАСС) и навигационным модулем. Как и любая другая радиостанция, работающая в этом частотном диапазоне, АИС-транспондер подвержен всем факторам, влияющим на передачу радиосигнала.
Вся информация автоматически отправляется в эфир посредством АИС-транспондера через равные определенные промежутки времени. Непосредственно система на судне состоит из следующих компонентов:
АИС-транспондера, который является и приемником, и передатчиком одновременно,
АФУ,
индикатора информации.

Дальность работы:

Дальность работы АИС-радиоприемника зависит от высоты расположения приёмной и передающей антенны, состояния среды распространения

радиоволн, встречающихся на пути преград и т.д. Тем самым дальность действия АИС-транспондера сопоставима с расстоянием работы судовой радиостанции в диапазоне 156-163 МГц и примерно равна 25-35 километрам.
Система увеличивает безопасность судовождения путем информирования судоводителей и всех заинтересованных лиц об обстановке в определенном секторе. Тем самым улучшается взаимодействие портовых служб, структур, отвечающих за безопасность на акватории, служб поиска и спасения, а также непосредственно экипажей судов.
АИС-транспондер не позволяет отображать и идентифицировать цели, которые не несут передатчик, работающий в системе АИС. Соответственно, совместное использование данных устройств на данный момент является оптимальным элементом системы освещения надводной обстановки.
Начиная с 2004 международная морская организация требует от всех судов путешествующих на международном уровне наличие транспондера класса АИС-А,который принимает и передает АИС данные. На бортах маленьких судов можно использовать транспондер класса АИС-В, который сам по себе проще и стоит меньше.

Виды АИС

Класс А | IEC 61993-2

Это судовое мобильное оборудование, предназначенное для удовлетворения эксплуатационных требований к перевозке, принятые Международной Морской Организацией (далее IMO). Станции класса А сообщают о своем местоположении автономно каждые 2-10 секунд в зависимости от скорости судна и / или изменения курса А также каждые три минуты или меньше, когда судно на якоре, или пришвартовано) Помимо этого передается статическая информация о рейсе. Каждые 6 минут. станции класса А способны обмениваться текстовыми сообщениями и информацией, связанной с безопасностью. Также передаются специальные сообщения-приложения погодных условий и дождя.

Класс В | IEC 62287-1 и 62287-2

Судовое мобильное оборудование, которое может взаимодействовать со всеми другими станциями АИС, но не отвечает всем эксплуатационным требованиям, принятым IMO. Подобно станциям класса А, они сообщают каждые три минуты или меньше, когда на якоре или пришвартованы, но их положение сообщается реже и при более низкой мощности. Кроме того, они сообщают статические данные судна каждые 6 минут, но не сообщают о своем рейсе. Они могут получить сообщение безопасности, но не могут его передать.

Поисково-спасательный для воздушных судов (стандарты IEC еще в разработке)

Созданный для малогабаритных самолетов. Как правило отчетность через каждые десять секунд.

AIS средство помощи в навигации (Aton) | IEC 62320-2

Береговая, или мобильная станция обеспечивающая определение местоположения и имеющая статус вспомогательного средства для навигации (ATON); который также может транслировать специальные сообщения приложения. Судно с таким статусом предназначено для собирания различной информации, такой как: метеорологические и гидрологические данные, В Соединенных Штатах, эти станции сообщают информацию о себе каждые три минуты, или меньше.

Передатчик АИС для целевого поиска и спасания | IEC 61097-14

Мобильное оборудование для оказания помощи на лодках и плотах. Используется для поиска выживших в море и людей за бортом.Такие передатчики работают на частоте 406 МГц.

Базовая станция АИС | IEC 62320-1

Береговая станция обеспечивающая идентичность и, синхронизацию времени, текстовых сообщений, которые также могут выступать в качестве станции AIS ATON, или передачу специальных сообщений приложений. В США используется исключительно береговой охраной. Такие станции обновляются каждые 10 секунд.

АИС транспондеры включают в себя GPS приемник, который собирает информацию о положении и перемещении судна, на регулярном промежутке времени с помощью встроенного передатчика ультракоротких волн с использованием 2 каналов (161.975 МГц и 162,025 МГц).

Периодически АИС-данные могут быть получены с других судов или базовыми станциями (при условии , что они находятся в пределах диапазона). Затем, с использованием специального программного обеспечения, они могут быть обработан и преобразован в изображение карты. К примеру по такой технологии работает сервис MarineTraffic. AIS-данные также могут быть получены с помощью спутников - в данном случае используется термин спутник АИС или S-AIS.

Возможности АИС

Увеличение общественного интереса к информации АИС привело к изменению первоначального восприятия ее использования. Первоначально АИС была разработана в качестве стандарта , который поможет судам избежать столкновения, а портовым властям регулировать морское движение с большей эффективностью. Тем не менее, стало ясно, что возможности АИС могут быть применимы к применению в сферах бизнеса.

В настоящее время информация АИС используется для достижения различных целей и облегчает работу людей различных профессий, таких, как: портовые власти, судовладельцы, строители, аналитики, буксиры, поисково-спасательные группы, агенты охраны окружающей среды и многих других.

АИС-принимающие станции

Практически, любой человек может установить и использовать приемную станцию. Но есть две важные детали - постоянная подача питания и стабильное подключение к интернету.

В большинстве случаев информация, полученная с АИС-транспондера, выводится на монитор в виде символов и отдельных таблиц. При наложении этих сведений на карту полученная навигационная обстановка представлена более полно и информативно.

Основные компоненты, необходимые для отслеживания судов это:

приемник АИС и антенна ультракоротких волн. Антенна принимает поступающую информации АИС, а АИС приемник способен обрабатывать эту информацию и отправить ее через интернет в базу данных , где она хранится и дополнительно обрабатывается таким образом , что информация может быть использована. Например, MarineTraffic, который собирает информацию из различных приемных станций в своей базе данных, и может отображать судна на карте.

Вы также можете использовать компьютер - оснащенный соответствующим программным обеспечением - для обработки входящих AIS-данных для использования и визуализации.

Морская безопасность

Благодаря неаутентифицированному и зашифрованному характера АИС данных, недавно доктор Марко Бадузи, Black Hat, и др. показали, что АИС является уязвимым для различных угроз, таких как спуфинг, угон данных и нарушения доступности.

На 79 сессии в декабре 2004 года Комитет по безопасности на море (Maritime Safety Committee, MSC) постановил, что, в связи с вопросом о свободном доступе к автоматизированной информационной системе (АИС) -сообщение данных корабля во всемирной сети, или в другом месте может нанести ущерб безопасности, охране судов и портовых средств и подрывает усилия Организации и ее государств-членов по повышению безопасности судоходства и безопасности в международном секторе морского транспорта.

Комитет осудил публикацию по всемирной сети, или в другом месте, данных AIS, передаваемых судов и настоятельно призвал членов-государств, при условии соблюдения положений своих национальных законов, не допускать публикацию АИС данных в открытом доступе.

Используемые источники:

ads-b.garmin.com/en-US
navcen.uscg.gov/?pageName=typesAIS
bit.ly/2hnxAyt
trueheading.se/en/ais-aton

Яковець Всеволод
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Одна зі стратегічних для будь-якої країни галузей – галузь телекомунікацій – відіграє величезну роль у збалансованому розвитку глобальної та регіональної економіки. Вона є з'єднувальною ланкою як промислової сфери, сфери послуг і споживачів, так і різних географічно розрізнених частин країни та економічних центрів. Стимулюючи людське спілкування за допомогою зв'язку, сучасні засоби телекомунікацій стають необхідною умовою для соціальної згуртованості та культурного розвитку всіх країн.

Наприкінці XX ст. – початку XXI ст. світ перебуває в стані інформаційної революції, вплив якої можна порівняти з впливом індустріальної революції минулого століття. Є всі підстави вважати, що обробка інформації – одна з найвагоміших складових економічної активності. Тому можна стверджувати, що розвиток телекомунікацій як важлива складова інформатизації суспільства та забезпечення населення високоякісними послугами зв'язку є одним з найважливіших напрямів національного та економічного розвтку будь-якої держави, і, зокрема, України.

Взагалі, характерною особливістю української телекомунікаційної галузі є значне відставання за часом по застосуванню нових технологій між Києвом та іншими регіонами країни. Наприклад, мобільний зв'язок у Харкові з'явився через 2-3 роки після його появи у Києві, а в деяких великих містах з населенням в 25 і більше тис. людей він відсутній і досі.

Станом на 1 квітня 2016 року, кількість активних SIM-карток в Україні зменшилась порівняно з 2015 роком на 3,6 млн. і становила 57,1 млн. штук, таким чином рівень проникнення мобільного зв'язку в Україні становив 133%. Це зумовлено популярністю мобільних телефонів з 2-ма SIM-картками. Реально користувачами мобільного зв'язку, за даними дослідження Київського міжнародного інституту соціології, на кінець 2013 року були 88% жителів країни. Крім мобільних телефонів сім-картки використовуються також в інших пристроях, які потребують зв'язку для передачі даних чи їх віддаленого

керування (наприклад різноманітні промислові датчики, сигналізації, термінали, тощо).

Україна також має великий і постійно зростаючий інтернет-сектор, а національний домен верхнього рівня (ccTLD) – .ua було зареєстровано 1 грудня 1992 року.

Згідно з даними Київського міжнародного інституту соціології (КМІС), у вересні 2013 року 49.8% дорослого населення України користувалися Інтернетом. Таким чином, зростання числа користувачів триває навіть більшими темпами, ніж це прогнозувалося. Темп приросту протягом лютого 2012 - жовтня 2013 років склав 16%, що трохи поступається рекордному стрибку в 34% у період з березня 2011 по лютий 2012 року.

Менш оптимістичну цифру 41,8% оприлюднив Міжнародний телекомунікаційний союз.

У сфері телекомунікацій України існують такі проблеми:

- низький рівень забезпечення населення, підприємств, установ і організацій широкосмуговими телекомунікаційними послугами;
- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах);
- неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- недостатній регуляторний вплив держави на ринок телекомунікацій;
- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій;
- низький рівень координації органами виконавчої влади діяльності з розвитку мереж загального користування;
- недосконалість нормативної бази з питань провадження інвестиційної діяльності;
- невідповідність системи нумерації телефонної мережі загального користування міжнародним та європейським вимогам;
- обмеженість вибору альтернативних мереж операторів телекомунікацій.

З метою прискорення розвитку телекомунікаційних мереж слід створити сприятливі умови для добросовісної конкуренції на ринку телекомунікаційних послуг, підвищити його інвестиційну привабливість, забезпечити прозорість взаємовідносин суб'єктів ринку телекомунікаційних послуг, консолідувати їх зусилля на розв'язання проблем розвитку телекомунікацій. Прискорений розвиток телекомунікацій є одним із основних чинників, що впливатиме на розбудову національної економіки та масове впровадження інформаційних технологій, побудову в Україні інформаційного суспільства, на процес інтеграції України в ЄС та у світову економіку, а також збільшення надходжень до державного бюджету.

Згідно з міжнародними деклараціями, які стосуються побудови інформаційного суспільства, перед Україною постає важливе завдання прискорити темпи розвитку національної інформаційної інфраструктури, узгодженої за принципами і органічно поєднаної з глобальною інформаційною інфраструктурою.

За принципами побудови глобальної інформаційної інфраструктури телекомунікації є її складовою, що забезпечує вільний рух інформації між її численними інформаційно-спеціалізованими складовими, такими як джерела і споживачі інформації, сховища та бази даних, переробники і розповсюджувачі інформації тощо. Телекомунікації повинні забезпечити безпеку і конфіденційність для користувачів, надання інфокомунікаційних послуг належної якості в будь-якому місці, будь-який час, за прийнятними цінами.

Використання Інтернет для розширення доступу до інфокомунікаційних послуг необхідно розглядати як умову інтеграції України у світовий інформаційний простір і розбудови інформаційного суспільства. У зв'язку з цим слід забезпечити надання державної підтримки розвитку Інтернет в Україні та стимулювати надання з використанням Інтернет таких послуг, як аудіо- та відеоспілкування, електронна освіта, електронна медицина, створення розподілених наукових мереж, електронне урядування, електронна торгівля тощо. Значну увагу слід приділяти розвитку всіх елементів телекомунікаційної інфраструктури українського сегмента Інтернет, що сприятиме розширенню номенклатури послуг та зниженню їх вартості у різних регіонах України.

Необхідно оптимізувати за вартісними і функціональними характеристиками телекомунікаційну інфраструктуру українського сегмента Інтернет (транзитні мережі Інтернет-трафіку, вузли міжмережних Інтернет-з'єднань, пункти обміну Інтернет-трафіком та вузли доступу до мереж транзиту Інтернет-трафіку, топологію з'єднань між основними інформаційними мережами тощо), знизити вартість міжмережевих з'єднань та доступу до транзитних мереж, стимулювати створення і розвиток телекомунікаційних

мереж, у тому числі на базі підприємств, організацій та житлово-комунальних об’єктів з використанням дротових і бездротових (радіо-) технологій.

Грищенко Ольга Юріївна
Журавель Катерина Ігорівна
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

АЛГОРИТМ І ЙОГО ЗНАЧЕННЯ В ІНФОРМАТИЦІ

Кожна людина використовує багато алгоритмів у їхньому житті, вони стають у нагоді для деяких задач, з якими люди зіштовхуються щоденно. Навіть проста програма, додавання, віднімання, множення — алгоритм і також розрахунок швидкості, шляху, палива космічного апарату робиться за допомогою алгоритмів. Ми використовуємо алгоритми щоб знайти найкоротший або кращий шлях для поїздки з одного розташування до іншого (Google Maps), прогнозування погоди, для знаходження структурних візерунків, виліковування недуг та для гри в шахи. Виділяти алгоритмічну суть явища та будувати алгоритми – дуже важливо для людини будь-якої професії.

***Мета** нашої роботи полягала у визначенні ролі та значення алгоритмів у житті людини.*

***Об’єктом дослідження** обрано алгоритм.*

***Предмет дослідження**— важливість алгоритмів у житті людини.*

***Завдання** роботи передбачали:*

1) *Порівняння викладання теми алгоритмів в інших ВУЗах Києва.*
2) *Зрозуміти та пояснити чому алгоритми відіграють важливу роль в нашому житті.*
3) *Ознайомитися з рішенням простої задачі.*

Основний матеріал статті: Сучасне суспільство називають інформаційним, адже сьогодні все базується на інформаційних технологіях. Кожна сфера життя людини залежить від машин, які певним чином запрограмовані. Але для того, щоб все працювало, є спеціалісти, які займаються програмуванням.

Якщо людина вибрала спеціальність пов’язану з інформаційними технологіями, то обов’язково вивчатиме інформатику, бо це є головною складовою навчального процесу. Предмет інформатика є дуже важливим для студентів 1 курсу тому, що вона має найширші застосування, яка охоплює всі види людської діяльності виробництво, управління, науку, освіту, проектні розробки, торгівлю, грошово-касові операції, медицину, криміналістику, охорону навколишнього середовища, мистецтвознавство, побут тощо.

Предмет інформатики визначається різноманітністю її застосувань. Інформаційні технології, що використовуються у різних видах людської діяльності (управління виробничим процесом, наукові дослідження, проектування, фінансові операції, освіта та інше), маючи спільні риси,в той самий час істотно відрізняються . Утворюються різні “ завдання ” інформатики, що базуються на різних операціях і процедурах, різних видах обладнання (в багатьох випадках на рівні з комп’ютером використовуються спеціалізовані прилади і пристрої,інформаційні носії тощо.

Щодо вивчення інформатики в інших Вищих Навчальних Закладах України можна сказати, що кожен з їх має свій план навчання, свої методи викладання, але основа все ж у будь – якому ВНЗ однакова. В Державному Університеті Телекомунікацій, інформатика вивчається більш поглиблено, кожна програма розглядається детально, для подальшого успіху студентів, адже майже всі спеціальності пов’язані , саме з інформаційними технологіями.

Інформатика стоїть на трьох китах — алгоритмізація, програмування та логіка. В цій схемі все взаємопов’язане. Між алгоритмами і програмами немає чіткого розмежування. Програмою зазвичай називають алгоритм вирішення задачі, розрахований на виконання його комп'ютером і записаний за допомогою пропозицій використовуваної мови програмування. Головна особливість всіх обчислень машини полягає в тому, що в основі її роботи лежить *програмний принцип керування*.Це означає, що для вирішення як найпростішої, так і найскладнішого завдання користувачеві необхідно використовувати перелік інструкцій або команд, слідуючи яким крок за кроком комп'ютер видасть необхідний результат. Таким чином, для того, щоб вирішувати завдання на ЕОМ, ЇЇ необхідно спочатку, як кажуть, алгоритмізувати. Саме алгоритмічний принцип і лежить в основі роботи всіх ЕОМ.

Одним з базових понять інформатики, обчислювальної техніки та програмування є поняття алгоритму, як деякого правила перетворення інформації. Уміння складати алгоритми і програми вирішення різних практичних завдань є елементом алгоритмічної культури сучасного фахівця в галузі інформаційних технологій. Знання теорії аналізу і алгоритмів застосовуються всіма програмістами насправді кожен день, просто ми звикли до цих речей настільки, що навіть не замислюємося над цим. Яке б завдання ви не вирішували - чи то простий сайт з вибіркою даних з бази, або скрипти на сервері, ви будете використовувати якісь структури даних. Алгоритми потрібні нам для того, щоб ефективно і з максимальними можливостями використовувати мову, на яких ви пишете. Щоб приймати поінформовані і осмислені рішення щодо вибору бібліотеки і технології для вирішення проблеми.Таким чином, інформатика - сьогодні це не тільки теорія інформаційного обміну, не тільки технологія обробки інформації та інформаційних потоків, це ціла соціально-технологічна інфраструктура , яка органічно переплітається з соціальною сферою і чинить на неї все більш істотний вплив. Інформаційні технологій дуже швидко перетворилися на

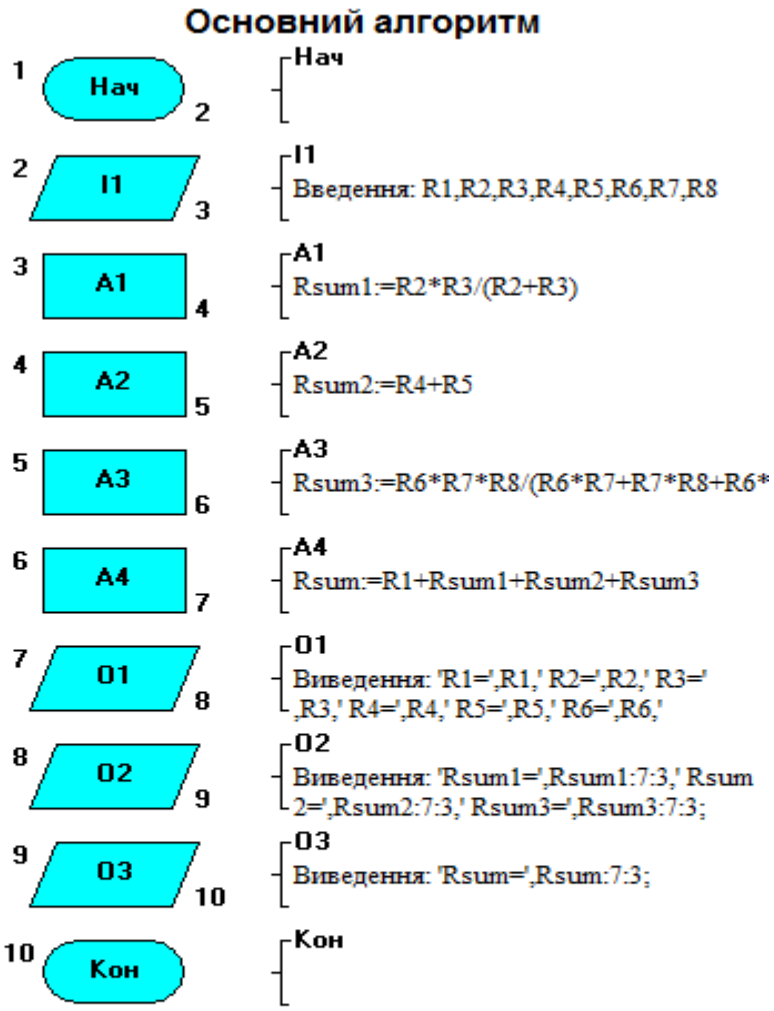
життєво важливий стимул розвитку не тільки світової економіки, а й інших сфер людської діяльності. На сьогодні практично неможливо знайти сферу, в якій зараз не використовуються інформаційні технології.

Не можливо оцінити важливість застосування інформаційних технологій у сфері освіти та науковій сфері. Зараз важко уявити собі школу, в якій би не було комп'ютерного класу, існує багато електронних бібліотек, користуватися якими можна не виходячи з дому, що значно полегшує процес навчання і самоосвіти. І при цьому інформаційні технології сприяють розвитку наукових знань.Збільшується швидкість обміну інформацією і з'являється можливість проводити складні математичні розрахунки за кільки секунд і багато іншого. Інформаційні технології це один із сучасних способів спілкування, головними перевагами якого є загальнодоступність.

В подальшому знання з інформатики потрібно застосовувати в своїй роботі, адже це є дуже важливо. Так в Україні налічуються сотні ІТ компаній, які певним чином пов'язані з інформатикою. Робота у цій сфері є вигідною, бо плата за послуги велика. І сьогодні на ринку праці не вистачає талановитих ІТ працівників. На нашу думку, з кожним роком попит на працівників у сфері ІТ зростає, світ змінюється, вводяться нові технології. Можливо в майбутньому ми матимемо такі технології, яка зараз нам здаються фантастикою, але завдяки винахідливості людей, ми змінюємо світ.

Алгоритми схожі на дорожню карту. Для досягнення пункту призначення потрібно чітко їхати по схемі. Для вирішення як найпростішої, так і найскладнішого завдання користувачеві необхідно використовувати перелік інструкцій або команд, слідуючи яким крок за кроком комп'ютер видасть необхідний результат

Розглянемо розробку та реалізацію простих лінійних алгоритмів. В якості приклада візьмемо блок-схему алгоритму розрахунку загального (сумарного) опору електричного ланцюга.



Змінні: r1:R=0.0, r2:R=0.0, r3:R=0.0, r4:R=0.0, r5:R=0.0, r6:R=
0.0, r7:R=0.0, r8:R=0.0, rsum1:R=0.0, rsum2:R=0.0, rs
m3:R=0.0, rsum:R=0.0,

Результат:

```
R1=1 R2=2 R3=3 R4=4 R5=5 R6=6 R7=7 R8=8
Rsum1=  1.200 Rsum2=  9.000 Rsum3=  2.301
Rsum= 13.501
```

Коли розроблений алгоритм виконання будь-якої задачі або проблеми, то виконання цього алгоритму більше не вимагає розуміння принципів на яких він був заснований. У зв'язку з цим рішення задачі або проблеми тепер можна звести до простого виконання певних кроків або слідування розробленим

раніше інструкцій. В якомусь сенсі, наш розум вимагає вирішувати проблеми у вигляді алгоритмів. Застосування алгоритмів дозволяє швидко вирішувати однотипні завдання, скоротити час на пошук рішення, автоматизувати процес його знаходження, а також поширювати знайдене рішення в стандартизованої - а значить, зрозумілою всім формі. І на останок, ви можете самі собі скласти надзвичайно складні алгоритми для контуру, енергії, палива. Як використовують індійські вчені щоб досягти Марсу з мінімальними витратами і найбільш ефективним способом.

***Висновки*:** Інформатика у світі телекомунікацій та інформатизації є головною складовою. Впровадження та вивчення цього предмету на 1 курсі Вищого Навчального Закладу - дуже важливо. Здобувати освіту за спеціальністю пов'язану з інформаційними технологіями вдалий крок, для людини, яка в майбутньому хоче стати успішною, та буде разом з іншими покращувати та полегшувати наше життя. Для кращого вивчення інформатики допоможуть алгоритми.

Список використаних джерел :
1.https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0
2. «Вікно в дивовижний світ інформатики» М. Г. Коляда.
3.http://ain.ua/it-kompanii-stali-liderami-top-20-samyx-uvazhaemyx-rabotodatelej-ukrainy

Андрієнко Олеся Григорівна,
Костюк Каріна Володимирівна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

ІНФОРМАТИКА - БАЗОВИЙ ПРЕДМЕТ ДЛЯ ВИВЧЕННЯ НА ПЕРШОМУ КУРСІ

Стаття присвячена висвітленню та аналізу необхідного матеріалу для вивчення на першому курсі предмету "Інформатика". Проаналізовано підходи різних ВУЗів щодо вивчення та впровадження цього напрямку. Розглянуто важливість вивчення алгоритмів для подальшого розвитку програмування, в тому числі системи Алгоритм.

Ключові слова: Інформатика, програмування, система Алгоритм.

Постановка проблеми. Процес дослідження інформатики, алгоритмів, базових навичок в програмуванні та їх теоретичних складових актуалізує широке коло професійних, методологічних і навчальних проблем, пов'язаних із пізнанням загальних закономірностей та структури розвитку наукового потенціалу і базових знань. Потужний внесок у розробку даної теоретичної проблематики було здійснено в рамках сучасних інформаційних технологій.

Йдеться, зокрема, про методологічне значення концепцій розвитку науки в напрямку інформаційних технологій, що на даний час має надзвичайно важливе значення при нинішньому розвитку технологій. Дана галузь суттєво рухається вперед і розвивається та дає нам нові уявлення про досягнення в науці, зокрема, в інформатиці. Тож можна сміливо сказати, що сьогодні без врахування наукового внеску, знання базових навичок з інформатики не може обійтись жодна серйозна робота. Оскільки зараз практично всюди використовується автоматика в управлінні і роботі найрізноманітніших систем і галузей, котрі побудовані і виконуються за певною програмою, яка в свою чергу працює за конкретним алгоритмом. Саме тому, **метою** статті є подальший розгляд предмету, який повинен викладатися з першого курсу та висвітлення позитивних аспектів даної теми.

Виклад основного матеріалу. В даній статті розглянемо декілька ключових питань, що пов'язані безпосередньо із впровадженням в систему навчання предмету і його вплив.

По-перше, що таке інформатика? Термін "інформатика" походить від французьких слів *information* (інформація) і *automatique* (автоматика) і дослівно перекладається як "інформаційна автоматика".

Інформатика - це заснована на використанні комп'ютерної техніки дисципліна, вивчаюча структуру і загальні властивості інформації, а також закономірності і методи її створення, зберігання, пошуку, перетворення, передачі і прийому в різних сферах людської діяльності. В 1978 році міжнародний науковий конгрес офіційно закріпив за поняттям "інформатика" області, пов'язані з розробкою, створенням, використанням і матеріально-технічним обслуговуванням систем обробки інформації, включаючи комп'ютери і їх програмне забезпечення, а також організаційні, адміністративні і соціально-політичні аспекти комп'ютеризації - масового впровадження комп'ютерної техніки у всі області життя людей. Таким чином інформатика базується на комп'ютерній техніці. Пріоритетні напрямки інформатики це:

- розробка обчислювальних систем і програмного забезпечення;
- теорія інформації, вивчаюча процеси, зв'язані з передачею, прийомом, перетворенням і зберіганням інформації;
- математичне моделювання, методи обчислювальної і прикладної математики;
- методи штучного інтелекту;
- системний аналіз;
- біоінформатика;
- соціальна інформатика;
- телекомунікаційні системи і мережі.

Перед програмуванням задачі завжди стоїть розробка способу її вирішення у вигляді послідовних дій, які ведуть від вихідних даних до шуканого результату, тобто розробка алгоритму вирішення задачі. В основі цього лежить вся суть вивчення предмету в цілому. Роль інформатики в розвитку суспільства надзвичайно велика. З нею пов'язаний початок революції в області накопичення, передачі і обробки інформації. Прогресивне збільшення можливостей комп'ютерної техніки, розвиток інформаційних мереж, створення нових інформаційних технологій приводять до значних змін у всіх сферах діяльності суспільства: в промисловості, науці, освіті, медицині - . Отож важливість вивчення цього предмету очевидна. Оскільки при вступі у ВУЗ, студент обирає певну спеціальність , яка пов'язана із інформаційними технологіями. Для початку формування свідомості про дану галузь, потрібно вводити цю дисципліну з першого курсу, щоб засвоїти початкові знання і уявлення про вибрану спеціальність. Оскільки на даний момент за світовою статистикою зарплата в сфері ІТ має перше місце, то вивчення цієї спеціалізації стоїть в пріоритеті. Як відомо технології зараз впроваджені в кожну систему роботи і знання та практичні навички у володінні комп'ютером мають декілька переваг. Вартість оплати за виконання роботи в будь-якій компанії значно більша за заробітну плату звичайних працівників, якщо перший володіє базовими знаннями інформатики. За підрахунками Держстату середня заробітна плата працівників інформаційної та телекомунікаційної галузей складає більше 7 тис. грн.

Для порівняння вивчення інформатики, то в більшості ВНЗ навчання закінчується на базових поняттях і програмах. Немає детального розгляду і заглиблення в зміст навчання. Якщо розглянути на прикладі передовий ВНЗ у сфері інформаційних технологій в Україні як Державний університет телекомунікацій, то інформатика викладається з першого курсу і вивчається поглиблено. Це дає змогу далі вивчати більш детально напрямки і розвивати свої навички.

Можна з впевненістю сказати, що вивчення предмету інформатики є важливим кроком у підготовці спеціалістів ІТ сфери.

По-друге, важливість вивчення алгоритмів вирішення задач перед вивченням мов програмування вищого рівня. Для початку, розглянемо поняття алгоритм детальніше. Багато хто вважає, що інформатика потрібна тільки для того, щоб навчитися працювати на комп'ютерах, але це не так. Для багатьох задач існують визначені правила (інструкції, команди), що пояснюють, як розв'язувати дану проблему. Саме слово алгоритм походить від algorithmi – латинської форми написання імені великого математика IX ст. Аль-Хорезмі, який сформулював правила виконання арифметичних дій.

Алгоритмом називають зрозуміле і точне розпорядження виконавцю про виконання послідовності дій, спрямованих на досягнення зазначеної мети чи на вирішення поставленої задачі. Поняття алгоритму в інформатиці є фундаментальним, тобто таким, котре не визначається через інші ще більш прості поняття. Алгоритмічне мислення допомагає чітко побачити кроки, що ведуть до мети, замітити всі перешкоди і уміло їх обійти. Основними властивостями алгоритму є:

- зрозумілість;
- визначеність;
- дискретність;
- масовість;
- результативність;
- ефективність.

Для роботи багатьох програм необхідно задавати початкові значення. Ці значення передаються в алгоритм за допомогою аргументів - .

Для прикладу розглянемо систему "Алгоритм", розроблену професором Мілєньким і доцентом Качановим. Система відноситься до складу автоматизованого візуального проектування і представляє собою інтегрований осередок, який дозволяє перетворювати, відображувати, налаштовувати і безпосередньо виконувати різні алгоритми. Використовується в навчальному процесі, професійному програмуванні, вирішенні широкого кругу обчислювальних задач. Для опису обчислювальних задач в Алгоритмі використовуються блоки, символи, дані вводу і виводу, цикли і процедури. Кожен блок характеризується набором параметрів. Застосування даної програми дає вагомий внесок у вивченні інформатики і подальшому вивченні мов високого рівня програмування.

Високорівнева мова програмування — мова програмування, розроблена для швидкого і зручного використання програмістом. Основна риса високорівневих мов — це абстракція, тобто введення смислових конструкцій, які коротко описують такі структури даних і операції над ними, опис яких на машинному

коді або низькорівневій мові програмування був би дуже великим, складним для розуміння програмістів і зайняв би багато часу при написанні - . Таким чином почати вивчення інформатики з більш простих програм буде доцільно і ефективно, адже вони дають фундамент в сприйнятті та в змозі самостійно вирішувати поставлені завдання. Це впливає також і на курс навчання предмету, адже інформація повинна бути подана в навчальному плані із наростанням складності завдань і програм. Ще одна перевага у початку вивченні інформатики на першому курсі.

По-третє, при отриманні необхідних знань, навиків і певного досвіду в роботі можна застосовувати їх в різних сферах. Як вже було сказано, спеціалісти в IT сфері найбільш затребувані і для цього велика маса підтверджень. Як повідомляє інформаційний портал програмістів і працівників сфери IT сайт DOU, заробітна плата на посаді DevOps за III квартиль складає 3000 доларів - [4]. Тому можна з впевненістю сказати, що навчання по курсу інформатики і подальший розвиток і ріст в даній галузі дає надзвичайно великі результати. Вивченні різних мов програмування дає можливість хорошого кар'єрного росту, це якщо говорити за фінансову сторону питання. На даний момент працівники IT цінуються в усіх сферах життя людини. Нові технології виникають постійно, як відомо кожні 6 років інформаційні технології повністю змінюються і виникають нові задачі. Спеціалістів потребують, які можуть швидко налагодити і мінімізувати затрати на роботу певної промисловості дуже цінуються. І тому вивчення інформатики було і буде дуже актуальним. На базових принципах роботи всіх систем є одні і ті ж правила роботи. Тому розпочинаючи із простих програм можна почати працювати над створення початкового проекту і потім тільки вдосконалювати його, застосовуючи більш високі технології, складніші процедури і алгоритми. Застосування знань в інформатиці можна відобразити і в покращені вже існуючих програм, створенню нових ідей і у вирішенні глобальних проблем. Навіть прості, на перший погляд, проблеми не можуть бути усунені за допомогою інформаційних технологій. Наведемо приклад більш масштабної події, яка відбулась зовсім нещодавно. Досить добре розвинена в технологіях країна, Японія запустила в космос вантажне судно із Міжнародної космічної станції, на борту якого знаходиться прибиральник "космічного сміття". За багато років відбулась велика кількість польотів в космос і виникала велика кількість "сміття", а саме 100 мільйонів різних уламків. Робота виконується завдяки алгоритм дій, закладеному і закодованому в системі судна .

Тож можна дійти висновку по цьому питанню, що застосувати свої можливості і отримані знання можливо в будь-якій сфері. Головне тільки мати бажання вчитись і йти до своєї мети . В цьому допоможе вивчення інформатики та подальший розвиток в цьому напрямку.

Розглянемо простий приклад використання програми Алгоритм в математиці. Завдяки правильному розрахунку і опису обчислювальної задачі знайдемо просте квадратне рівняння.

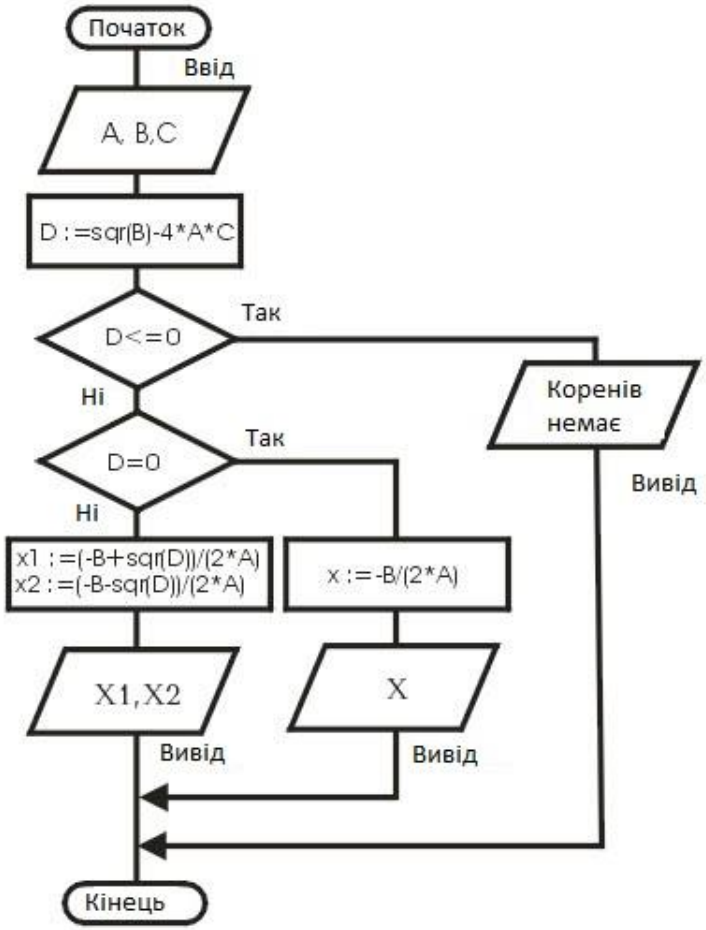


Рисунок 1. Квадратне рівняння в системі Алгоритм.

Таким самим чином виконуються і решта завдань, від простого до складного.

Висновки. Враховуючи вище сказане, можна підвести загальні підсумки стосовно даної теми. Впровадження в систему навчання у вищих навчальних закладах такого предмету як "Інформатика" на першому курсі є досить вдалим кроком до поліпшення вивчення як свої спеціальності так і покращення рівня своєї освіти студентами. Цю методику, на нашу думку, потрібно застосовувати, адже ми живемо в інформаційному суспільстві і це є одним і вагомих аспектів нашого життя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації з дисципліни "Інформатика" для 1 курсу, Державний університет телекомунікацій.
2. Інформатика [Електронний ресурс] // Поняття алгоритмів, властивості алгоритмів - Режим доступу: https://stboinf.wordpress.com/2013/03/14/%D0%BF%D0%BE%D0%BD%D1%8F%D1%82%D1%82%D1%8F-%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D1%83-%D0%B2%D0%BB%D0%B0%D1%81%D1%82%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D1%96-%D0%B0%D0%BB%D0%B3%D0%BE%D1%80/.
3. Wikipedia [Електронний ресурс] // Мова програмування високого рівня - Режим доступу: https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B2%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B2%D0%B8%D1%81%D0%BE%D0%BA%D0%BE%D0%B3%D0%BE_%D1%80%D1%96%D0%B2%D0%BD%D1%8F.
4. DOU [Електронний ресурс] // Статистика зарплат програмістів в Україні - Режим доступу: https://jobs.dou.ua/salaries/#period=may2016&city=Kyiv&title=DevOps&language=&spec=&exp1=0&exp2=10.
5. hi-news.ru [Електронний ресурс].
6. Программирование алгоритмов с ветвящейся структурой [Електронний ресурс] - Режим доступу: http://www.kolomna-school7-ict.narod.ru/st60402.htm.

Гнотівський Едуард Віталійович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

ОПТИЧНЕ ВОЛОКНО ЯК КРОК В МАЙБУТНЄ

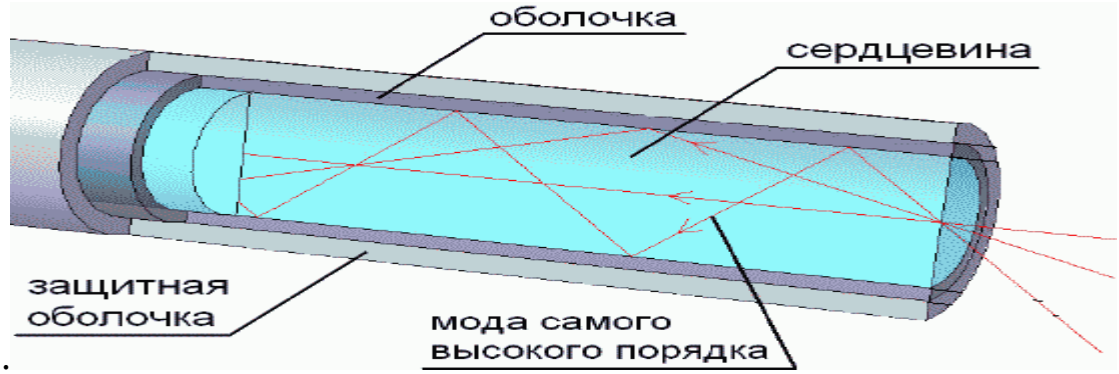
Оптичне волокно в даний час вважається найдосконалішою фізичним середовищем для передачі інформації, а також самим перспективним середовищем для передачі великих потоків інформації на значні відстані. Підстави так вважати випливають із ряду особливостей, притаманних оптичним хвилеводам.

1.Оптичне волокно - нитка з оптично прозорого матеріалу (скло, пластик), використовувана для перенесення світла всередині себе за допомогою повного внутрішнього відображення.

1.1 Технічні особливості

Волокно виготовлене з кварцу, основу якого складає двоокис кремнію, широко поширеного, а тому недорогого матеріалу, на відміну від міді.

Оптичне волокно має круглий перетин і складається з трьох частин – серцевини, оболонки і захисної оболонки (Рис.1). Для забезпечення повного внутрішнього відображення абсолютний показник заломлення серцевини трохи вище показника заломлення оболонки. Наприклад, якщо показник заломлення оболонки дорівнює 1,474, то показник заломлення серцевини -

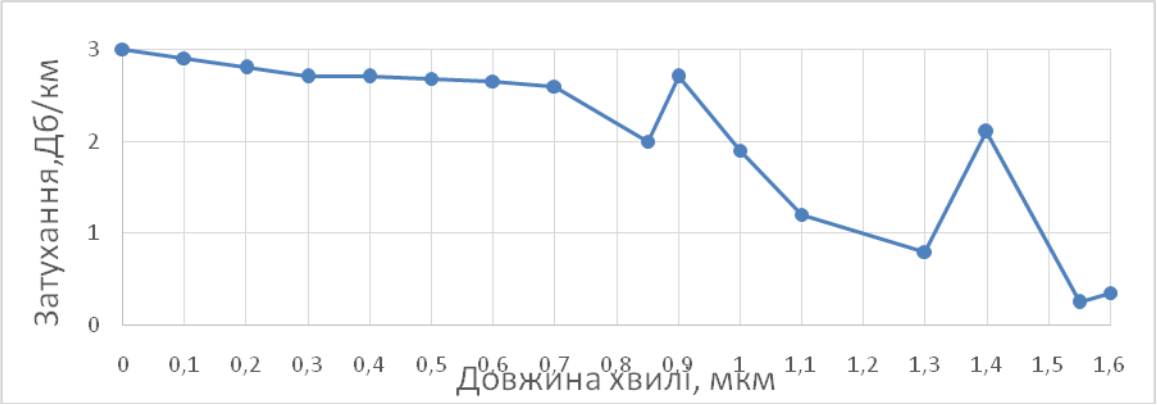


1,479.

Рис.1

Промінь світла, спрямований у серцевину, буде поширюватися по ній, відчуваючи багаторазові перевідбиття від кордону розділу «серцевина - оболонка».

Втрати на поглинання залежать від чистоти матеріалу, втрати на розсіювання залежать від неоднорідностей показника заломлення матеріалу.



Загасання залежить від довжини хвилі випромінювання, що вводиться у волокно. В даний час передачу сигналів по волокну здійснюють в трьох діапазонах: 0.85 мкм, 1.3 мкм, 1.55 мкм, так як саме в цих діапазонах кварц має підвищену прозорість.

Усі оптичні волокна, використовувані в телекомунікаціях, мають діаметр 125 ± 1 мікрон тобто дуже компактні і легкі, що робить їх перспективними для використання в авіації, приладобудуванні, в кабельній техніці.

Діаметр серцевини може відрізнятися в залежності від типу волокна і національних стандартів.

Скляні волокна - не метал, при будівництві систем зв'язку автоматично досягається гальванічна розв'язка сегментів. Застосовуючи особливо міцний пластик, на кабельних заводах виготовляють самонесучі підвісні кабелі, що не містять металу і тим самим безпечні в електричному відношенні. Такі кабелі можна монтувати на щоглах існуючих ліній

електро-передач, як окремо, так і вбудовані в фазовий провід, економлячи значні кошти на прокладку кабелю через річки та інші перешкоди.

Системи зв'язку на основі оптичних волокон стійкі до електромагнітних перешкод, а передається по світловода інформація захищена від несанкціонованого доступу. Волоконно-оптичні лінії зв'язку не можна підслухати неруйнуючим способом. Всякі впливи на волокно можуть бути зареєстровані методом моніторингу (безперервного контролю) цілісності лінії. Теоретично існують способи обійти захист шляхом моніторингу, але витрати на реалізацію цих способів будуть настільки великі, що перевершать вартість перехопленої інформації.

Існує спосіб прихованої передачі інформації по оптичних лініях зв'язку. При прихованої передачі сигнал від джерела випромінювання модулюється не по амплітуді, як у звичайних системах, а по фазі. Потім сигнал змішується з самим собою, затриманим на деякий час, більший ніж час когерентності джерела випромінювання.При такому способі передачі інформація не може бути перехоплена амплітудним приймачем випромінювання, так як він зареєструє лише сигнал постійної інтенсивності.

Для виявлення перехоплюємого сигналу знадобиться перебудовуючи інтерферометр Майкельсона спеціальної конструкції. Причому, видність інтерференційної картини може бути ослаблена як 1:2N, де N - кількість сигналів, одночасно передаються по оптичній системі зв'язку. Можна розподілити передану інформацію з безлічі сигналів або передавати декілька шумових сигналів, погіршуючи цим умови перехоплення інформації. Буде потрібно значний відбір потужності з волокна, щоб несанкціоновано прийняти оптичний сигнал, а це втручання легко зареєструвати системами моніторингу.

1.2 Фізичні процеси в оптичних волокнах

Оптичний зв’язок в закритому середовищі(по світловодам і оптичним кабелям) відноситься до області передачі енергії по направляючим системам хвилеподібним методом.

(Рис.2). Схематичне зображення розповсюдження лазерного променя в світловоді:

а) – короткі хвилі (λ – 0); б) - хвилі, які співрозмірні з з діаметром осердя (λ ---d);

в) критичні хвилі (λ o = d, f o = c/ λo = c/d).

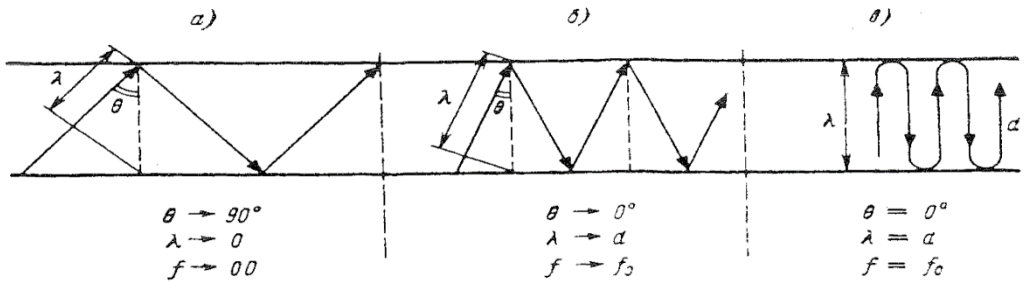


Рис.2

При довжині хвилі світлового променю λ < d – розміру поперечного перерізу оптичного резонатора не вимагається двохпроводової системи, а передача енергії відбувається за рахунок багаторазового зигзагоподібного відбивання хвилі від границі розділу діелектриків з різними оптичними характеристиками.

Основним елементом оптичного кабелю (ОК) є волоконний світловод, виготовлений у вигляді скляного волокна циліндричної форми. Волоконний світловод має двохшарову конструкцію і складається з серцевини і оболонки з різними оптичними характеристиками – показниками заломлення n1 і n2. Осердя слугує для передачі електромагнітної енергії. Призначення оболонки: створення кращих умов відбивання на границі розділу осердя – оболонка і захист від розсіювання енергії в навколишній простір. На зовнішній стороні кабелю знаходиться захисне покриття для захисту волокна від механічних впливів і нанесення розмітки. Передача хвилі по світловоду здійснюється за рахунок відбиття її від границі розділу осердя – оболонка, які мають різні показники заломлення (n1 > n2). В проводових кабелях зв’язку носієм інформації, що передається, є електричний струм, а в ОК – лазерний промінь певної довжини хвилі.

Найбільш широке застосування в лініях передачі інформації отримали волоконні світловоди двох типів: сходинкові і градієнтні (див. Рис. 3). У сходинкових світловодах показник заломлення в осерді має постійне значення і має різкий перехід від n1 осердя до n2 оболонки. В них промені зигзагоподібно відбиваються від границі розділу осердя – оболонка.

Рис.3. Схеми розповсюдження електромагнітних хвиль в оптичних кабелях:

а) з сходинковою дисперсією, б) з градієнтною дисперсією показника заломлення.

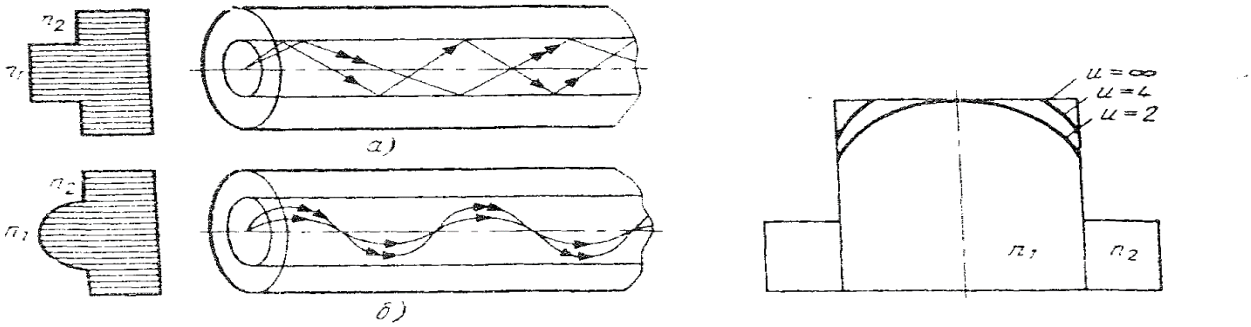


Рис.3Градієнтні світловоди мають показник заломлення n1, який неперервно змінюється в осерді по радіусу від центра до периферії, при цьому промені поширюються в ньому по хвилеподібній траєкторії. Показник заломлення осердя змінюється по закону показникової функції:

$$n_r = n_0 \left[1 - 2\Delta \left(\frac{r}{a}\right)^u\right]^{\frac{1}{2}}$$

де n_0 – максимальне значення показника заломлення на осі волокна, тобто при r = 0;

а – радіус осердя оптичного світловода; и – показник ступеню, який описує профіль зміни показника заломлення , а параметр Δ визначається за формулою:

$\Delta = \frac{n_1^2 - n_2^2}{2\ n_1^2} \approx \frac{n_1 - n_2}{n_1} = 0{,}003 - 0{,}01$.Частіше всього застосовуються світловоди з параболічним профілем (и = 2) і відповідно:

$$n_r = n_0 \left[1 - 2\Delta \left(\frac{r}{a}\right)^2\right]^{\frac{1}{2}}$$

Для попередження переходу енергії в оболонку і випромінювання в навколишнє середовище необхідно забезпечити умову повного внутрішнього відбиття під кутом Θ :

$$\sin\theta_B = \frac{n_2}{n_1} = \sqrt{\frac{\mu_2 \varepsilon_2}{\mu_1 \varepsilon_1}}$$

де μ1 і ε 1 – магнітна і діелектрична проникності осердя, а μ2 і ε 2 - оболонки.

Режим повного внутрішнього відбивання визначає умову попадання світла на вхідний торець волоконного світловоду. Світловод пропускає лише світло, яке розповсюджується в межах тілесного кута Θ_A, який називається апертурою: кут між оптичною віссю і одним із утворюючих

променів конуса, для якого виконується умова повного внутрішнього відбиття. Завжди користуються поняттям числової апертури (ε о = 1 для повітря) :

$$NA = \sin\theta_A = \sqrt{n_1^2 - n_2^2}$$

Розглянемо критичні частоти і довжини хвиль волоконних світловодів, які можна передавати. З Рис. 19 видно, що λ і d звязані між собою: λ = d cos Θ = d √ 1 – (n1/ n2) ^{2}

Отже:$\frac{\lambda_0}{d} = \sqrt{1 - \left(\frac{n_2}{n_1}\right)^2}$

Звідси визначимо критичну довжину світлової хвилі λ_0:

$$\lambda_0 = d\sqrt{1 - \left(\frac{n_2}{n_1}\right)^2} = \frac{d}{n_1}\sqrt{n_1^2 - n_2^2}$$

Критична частота (частота відсічки) визначається за формулою :

$$I_0 = \frac{u_1}{\lambda_0} = \frac{u_1}{d}\frac{1}{\sqrt{1 - \left(\frac{n_2}{n_1}\right)^2}} = \frac{c}{d}\frac{1}{\sqrt{n_1^2 - n_2^2}}$$

де υ1 – швидкість поширення хвилі в осерді, а с – швидкість світла у вакуумі,n 1 і n 2 – показники заломлення світла в осерді і оболонці, відповідно.

Аналізуючи отримані співвідношення можна помітити, що чим більший діаметр серцевини волоконного світловоду d і чим більше відрізняються показники заломлення осердя і оболонки, тим більша критична довжина хвилі і менша критична частота. Можна зробити висновок, що при частотах більших за критичну вся енергія поля концентрується всередині осердя світловоду і ефективно розповсюджується вздовж нього. Нижче критичної частоти енергія розсіюється в навколишньому просторі і не передається по світловоду.

Література:

1. http://www.network.xsp.ru/5_6.php#1
2. Михайло Цибін.Волоконная оптика
3. Скляров О.К. Волоконно-оптичні мережі та системи зв'язку
4. Листвин А.В., Листвин В.Н., Швырков Д.В.Оптичні волокна для ліній зв'язку.

Гнотівський Едуард Віталійович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

ОПТИЧНІ З'ЄДНАННЯ

З'єднання оптичних волокон між собою, під'єднання їх до обладнання, строго кажучи, не є окремим компонентом ВОСП. Однак з огляду на те, що вони суттєво впливають на величину загасання регенераційної дільниці, а відсутність належної уваги до їх якості і правильності застосування може в декотрих випадках зробити неможливим або створити перепони в експлуатації встановлює мого обладнання ВОСП і спричинити до необхідності перемонтажу муфт або заміни з'єднувальних елементів в оптичних кросах, їх можна розглядати як компонент ВОСП.

Після того, як оптичний кабель прокладений, необхідно з'єднати його з приймально-передавальною апаратурою. Зробити це можна за допомогою оптичних конекторів(з'єднувачів). В системах зв'язку використовуються конекторибагатьох видів.

Оптичні з'єднувачі поділяються на роз'ємні та нероз'ємні. Роз'ємні пристрої призначені для швидкого та надійного багатократного з'єднання та роз'єднання різних компонентів волоконно-оптичних ліній.

Конструкція роз'ємного з'єднувача містить три елементи – два штекера (армовані ВС з накидними гайками) та перехідну розетку

Конектори також використовують у виробництві оптичних шнурів різної довжини (частіше довжиною 1 ÷ 3 метра) що використовуються для підключення вимірювального обладнання до оптичних кросів або портів обладнання ВОСП до оптичних кросів, з'єднання оптичних кросів між собою і т. д.)

В загальному без конекторів,робота з оптичними волокнами була меншпродуктивною і дорожчою у використанні, що ускладнювало б використання самих волоконно-оптичних систем.

Література:
1.http://www.network.xsp.ru/5_6.php#1
2 Скляров О.К.Волоконно-оптичні мережі та системи зв'язку

Ковальов Сергій Ігорович
Державний Університет Телекомунікацій
Факультет телекомунікацій
м. Київ

ВАЖЛИВІСТЬ ПРЕДМЕТА ИНФОРМАТИКА НА ПЕРШОМУ КУРСІ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Дослідження показують, що в останнє десятиліття інформатика як фундаментальна наука стає ключовою складовою всієї системи наукового пізнання і буде в значній мірі визначати шляхи формування глобального інформаційного суспільства, заснованого на знаннях. У зв'язку з цим цілком зрозумілий той підвищений інтерес до проблеми уточнення місця інформатики в системі наук, а також до її фундаментальних основ, історико-філософським, науково-методологічним і соціально-культурологічним аспектам, який спостерігається сьогодні як в сфері науки, так і в сфері освіти.Інформатика - це наукова дисципліна про закономірності перебігу інформаційних процесів в різних середовищах, а також про методи і засоби їх автоматизації.

Інформатика закладає основу створення і використання інформаційних та комунікаційних технологій (ІКТ) - одного з найбільш значущих технологічних досягнень сучасної цивілізації. На сьогоднішній день ІКТ - необхідний інструмент практично будь-якої діяльності.

Інформатика, ІКТ істотно впливають на світогляд і стиль життя сучасної людини. Суспільство, в якому вирішальну роль відіграють інформаційні процеси, властивості інформації, ІКТ - реальність теперішнього часу.

Інформатика має дуже велике і все зростаюче число міждисциплінарних зв'язків. Можна сказати, що вона являє собою метадисципліну, що має загальнонаукову мову.

На особливу увагу заслуговують міждисциплінарні зв'язки математики та інформатики. Ці дисципліни не є конкуруючими. При цьому інформатика не є частиною математики, хоча ряд понять може бути одночасно віднесений до компетенції обох дисциплін. Більш продуктивно розглядати математику і інформатику як дисципліни, в певній мірі доповнюючі один одного.

В інформатиці формуються багато видів діяльності, які мають загально-дисциплінарний характер: моделювання об'єктів і процесів, збирання, зберігання, перетворення і передача інформації, управління об'єктами і процесами. Особливість інформатики полягає в тому, що значна частина цієї діяльності може бути здійснена за допомогою комп'ютерних інструментів.

Основні цілі вивчення інформатики:

- Освоєння знань, що складають основу наукових уявлень про інформацію, інформаційні процеси, системи, технології і моделі.
- Розвиток пізнавальних інтересів, інтелектуальних і творчих здібностей засобами ІКТ.
- Виховання відповідального ставлення до інформації з урахуванням правових і етичних аспектів її поширення; вибіркового ставлення до отриманої інформації.
- Оволодіння вміннями працювати з різними видами інформації з допомогою комп'ютера та інших засобів ІКТ, організовувати власну інформаційну діяльність і планувати її результати.
- Вироблення навичок застосування засобів ІКТ у повсякденному житті, при виконанні індивідуальних і колективних проектів, в навчальній діяльності, при подальшому освоєнні професій, затребуваних на ринку праці.

Зміст курсу:

- Загальні поняття (в тому числі одиниці виміру інформації, інформаційні процеси, властивості інформації).
- Цінність інформації (в т.ч. формалізація завдання, комп'ютерне моделювання).
- Математичні поняття (в т.ч. алгоритми, системи числення, основи логіки).
- Характеристики комп'ютера (основні компоненти комп'ютера і їх функції, програмний принцип роботи комп'ютера, комп'ютерні мережі, склад і функції програмного забезпечення, мови програмування і реалізація алгоритмів).
- Інформаційні технології (введення інформації, обробка текстів, зображень, звуку і відео, використання готових шаблонів і бібліотек, організація і пошук інформації, проектування і моделювання, інформаційне середовище комунікації і взаємодії, ІКТ в суспільстві)

ВАЖЛИВІСТЬ ПРЕДМЕТУ ИНФОРМАТИКА НА ПЕРШОМУ КУРСІ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Виключно велика роль інформатики в підготовці студентів до праці, професійної діяльності, професійному самовизначенні молоді.

В даний час в Україні, як і у всіх розвинених країнах світу, почався поступовий перехід до постіндустріального, так званого, "інформаційного" суспільства. Відмінною рисою постіндустріального етапу розвитку є перенесення центру ваги в суспільному розподілі праці зі сфери матеріального виробництва в область інформаційних процесів і технологій, т. Е. Зміна домінуючого виду діяльності людини, обумовленого переходом від індустріального до інформаційного етапу розвитку суспільного виробництва. Це призводить до нового розуміння готовності випускників навчальних закладів до життя і праці в інформаційному суспільстві, змушує переосмислити традиційні уявлення про зміст освіти, шляхи його здійснення

Аналіз змісту професійної діяльності людей масових професій і, особливо, прогноз її розвитку в найближчій перспективі дозволяють зробити висновок про зростання ролі підготовки молоді в галузі інформатики та інформаційних технологій.

Зростаюче значення інформаційної діяльності впливає на перерозподіл в структурі робочих місць: відбувається "перекачування" трудових ресурсів з матеріальної сфери в інформаційну, з'являються нові професії, безпосередньо пов'язані з обробкою інформації.

В даний час в розвинених країнах число людей, зайнятих сільськогосподарським виробництвом не перевищує 4% працездатного населення, робітники промислових спеціальностей складають близько 16%, а так звані "інформаційні" працівники (т. Е. Ті, у кого обробка інформації - основний вид професійної діяльності) - приблизно 60%.

Таким чином, інформаційна частина стає провідною складовою технологічної підготовки людини, в якій би сфері діяльності їй не довелося працювати в майбутньому.

Особливо слід відзначити важливість початкової підготовки в галузі управління. Як відомо, багато розвинені в технологічному відношенні країни (Великобританія, ФРН і ін.) бачать в цьому запоруку успішного державного і економічного розвитку.

Спочатку мета навчання інформатики у вищих навчальних закладах була сформульована таким чином: формування первинних уявлень про властивості інформації, способах роботи з нею, зокрема з використанням комп'ютера

Для досягнення поставленої мети планувалося вирішити такі завдання: познайомити студентів з основними властивостями інформації, навчити їх прийомам організації інформації та планування діяльності, зокрема навчальної,

при вирішенні поставлених завдань; дати студентам початкові уявлення про комп'ютер і сучасні інформаційні і комунікаційні технології; дати студентам уявлення про сучасне інформаційне суспільство, інформаційної безпеки особистості і держави.
Основні поняття інформатики. Інформація та її властивості: сенс, опис, оцінка. Роль людини в перетворенні інформації і створенні нової інформації. Обробка, передача, зберігання інформації за допомогою технічних пристроїв. Види інформації: текст, число, зображення, звук. Способи організації інформації: таблиці, схеми, каталоги та ін. Організація діяльності людини по перетворенню інформації. Поняття про алгоритм. Властивості алгоритму. Виконавець алгоритму. Команди. Приписи. Приклади алгоритмів.

ВАЖЛИВІСТЬ ВИВЧЕННЯ АЛГОРИТМІВ (В Т.Ч. СИСТЕМИ АЛГОРИТМ) ДО ВИВЧЕННЯ МОВ ВИСОКОГО РІВНЯ І ОБ'ЄКТОВОГО ПРОГРАММИРОВАНИЯ

Перший крок до розуміння важливості вивчення і знання алгоритмів це дати точне визначення того, що розуміється під алгоритмом. Згідно популярній книзі Алгоритми: побудова й аналіз (Кормен, Лейзерсон, Ривест, Штайн) «алгоритм (algorithm) - це будь-яка коректно певна обчислювальна процедура, на вхід (input) якої подається деяка величина або набір величин, і результатом виконання якої є вихідна (output) величина або набір значень ». Іншими словами, алгоритми схожі на дорожні карти для досягнення чітко визначеної задачі. Шматок коду, для обчислення членів послідовності Фібоначчі - це реалізація конкретного алгоритму. Навіть проста функція складання двох чисел є алгоритмом, хоча і простим.

Деякі алгоритми, наприклад, для обчислення послідовності Фібоначчі, є інтуїтивно зрозумілими і відносяться до вроджених навичкам логічного мислення і розв'язання задач. Проте, більшості з нас буде не зайвим вивчити і складні алгоритми, щоб в майбутньому можна було використовувати їх в якості будівельних блоків для більш ефективного вирішення логічних завдань. Насправді можна здивуватися, дізнавшись як багато складних алгоритмів використовується людьми при перевірці електронної пошти або слуханні музики. У цій статті представлені деякі основні ідеї аналізу алгоритмів з практичними прикладами, що ілюструють важливість вивчення алгоритмів.

Аналіз часу виконання алгоритму. Одним з найбільш важливих аспектів алгоритму є його швидкість. Часто буває легко придумати алгоритм вирішення завдання, але якщо алгоритм занадто повільний, то він повертається на доопрацювання. Оскільки точна швидкість алгоритму залежить від того де запускається алгоритм, а також деталей реалізації, комп'ютерні фахівці зазвичай говорять про час виконання щодо вхідних даних.

Проте, час виконання багатьох складних алгоритмів залежить не тільки від розміру вхідних даних, але і від безлічі інших чинників. Наприклад, алгоритм сортування безлічі цілих чисел може працювати набагато швидше, якщо це безліч вже відсортована. Прийнято говорити про найгірший випадок виконання, і середній випадок виконання. Найгірший час виконання - це максимальний час роботи алгоритму при самому «поганому» його усіх можливих входів.

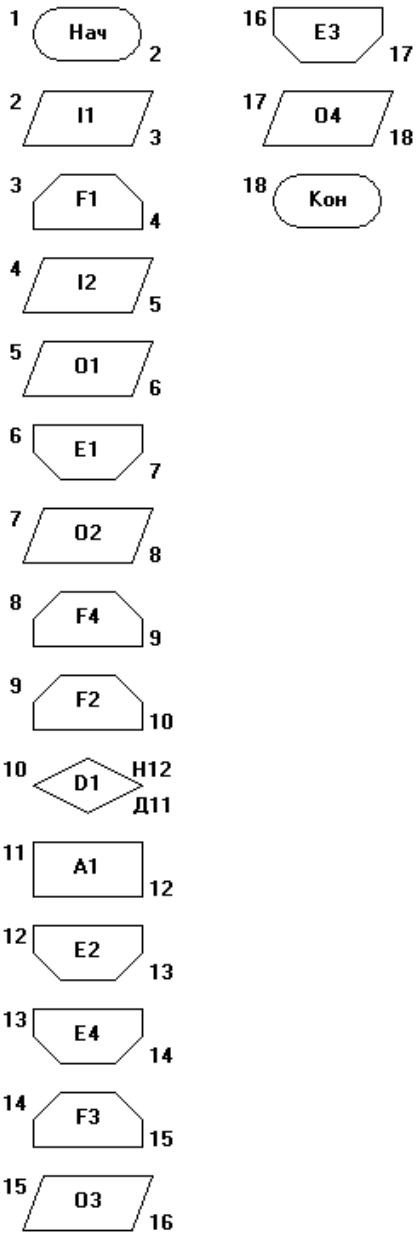
Середній випадок виконання - це середній час роботи алгоритму на всіх можливих входах. Із цих двох типів часу виконання, найлегше міркувати про найгірший випадок і тому його використовують частіше за зразок для заданого алгоритму. Процес визначення найгіршого і середнього випадку часу виконання алгоритму може бути досить складним, тому що зазвичай неможливо запустити алгоритм для всіх можливих входів.

ДЕ ОЧІКУЄТЬСЯ МОЖЛИВЕ ЗАСТОСУВАННЯ ОТРИМАНИХ ЗНАНЬ І НАВИЧОК

Сучасний урок неможливий без високої навчально-пізнавальної активності учня. У зв'язку з цим одним із прийомів навчання є використання на уроках різних способів алгоритмізації. Останнім часом широкого поширення набули пам'ятки - алгоритми, що орієнтують учнів на відбір і послідовний виклад матеріалу з тієї чи іншої теми. При правильному застосуванні пам'ятки її питання як би ведуть учнів від вивчення зовнішньої сторони явищ до пізнання їх сутності, допомагають розділити процес пізнання на етапи, чітко ставлять цілі кожного етапу пізнання, поєднують вимоги діалектики з завданнями конкретно-історичного аналізу і узагальнення. Алгоритми нами широко застосовуються при вивченні хімії, біології, математики і в основному інформатики.

Таким чином, використання алгоритмів допомагає учням опанувати логікою алгоритмічного мислення, порівнювати, узагальнювати, аналізувати матеріал, розвивати самостійність і творчість. Робота з алгоритмами сприяє формуванню навичок навчально-пізнавальної компетентності учнів. Використання алгоритмів в практиці викладання методично виправдано і особисто значуще для учнів.

Задача:Дано масив А, що складенз n елементів – чисел, розміщених у вільному порядку. Потрібновпорядкуватиелементимасива по спаданню.



Основний алгоритм

Нач

I1
Введення: n

F1
Поч. циклу 1: i:=1 to n

I2
Введення: x[i]

O1
Виведення: ' x[',i,'] = ', x[i]:6:3

E1
Кін. циклу 1:

O2
Виведення: ;

F4
Поч. циклу 4: J:=1 to n

F2
Поч. циклу 2: i:= 1 to (n-1)

D1
x[i]< x[i+1]

A1
a:= x[i]; x[i]:=x[i+1];x[i+1]:=a

E2
Кін. циклу 2:

E4
Кін. циклу 4:

F3
Поч. циклу 3: i:=1 to n

O3
Виведення: ' x[',i,'] = ', x[i]:6:3

E3
Кін. циклу 3:

O4
Виведення: ;

Кон

Результат:

```
x[1] =  6.000 x[2] =  4.000 x[3] =  9.000 x[4] =  7.000 x[5] =  8.000
x[1] =  9.000 x[2] =  8.000 x[3] =  7.000 x[4] =  6.000 x[5] =  4.000
```

Література:

1. *Колин К.К.* Становление информатики как фундаментальной науки и комплексной научной проблемы. Сб. н. тр. //Системы и средства информатики. Спец. вып. Научно-методологические проблемы информатики. –М.: ИПИ РАН, 2006. – С.7-57.
2. *Колин К.К.* Эволюция информатики. // Информационные технологии, № 1, 2005. – С. 2-16.
3. *Колин К.К.* Фундаментальные проблемы информатики. Сб. н. тр. «Системы и средства информатики». Вып. 7. – М.: Наука, 1995. – С. 5-20.

4. *Ершов А.П.* Информатика: предмет и понятие. В кн. Кибернетика. Становление информатики. – М.: Наука, 1986. – С. 28-31.

Любімов Дмитро Андрійович,
Висоцький Олег Віталійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОБРОБКИ ДАНИХ У СИСТЕМІ УПРАВЛІННЯ

Отримання великих обсягів інформації перетворюється для фахівців з інформатики та менеджерів у серйозну проблему. Для того, щоб ідентифікувати тільки необхідну інформацію для вирішення якоїсь конкретної задачі, доводиться "перебирати" величезна кількість даних.Дані - це "сирі" факти і цифри, в яких немає нічого особливого і які самі по собі не можуть бути корисними для менеджерів. Для того щоб витягти корисну інформацію, необхідно обробити, отримати закінчений • інформаційний продукт, що має безпосереднє відношення до управлінської задачі. Проблема ефективної ідентифікації корисної інформації та забезпечення доступу до неї менеджерів і співробітників набуває все більшої гостроти.

Про значення даної проблеми свідчить той факт, що в багатьох організаціях вводиться посада головного спеціаліста з інформації, який несе відповідальність за управління організаційними базами даних та впровадження нових інформаційних технологій. Як правило, фахівці з інформації стикаються з проблемою вибору одного з безмежного безлічі варіантів придбання апаратного та програмного забезпечення, мережевого і телекомунікаційного устаткування. Обсяг даних, які здатні давати комбінації цих технологічних засобів в рівній мірі, величезний. Прийняття рішень, пов'язаних із застосуванням нових технологічних засобів та управлінням їх ресурсами, часто лягає насамперед на плечі головного спеціаліста з інформації. Йому доводиться інтегрувати поточні та нові технології підтримки прийняття організаційних рішень, забезпечення операційних процесів і комунікацій так, щоб співробітники організації отримували необхідну інформацію в потрібному місці в потрібний час.

Інформаційна технологія обробки даних призначена для розв'язання добре структурованих задач, по яких є необхідні вхідні дані і відомі алгоритми та інші стандартні процедури їх опрацювання. Ця технологія застосовується на

рівні операційної (виконавчої) діяльності персоналу невисокої кваліфікації з метою автоматизації деяких постійно повторюваних операцій управлінської праці. Тому впровадження інформаційних технологій і систем на цьому рівні істотно підвищить продуктивність праці персоналу, звільнить його від рутинних операцій, можливо, навіть призведе до необхідності скорочення чисельності працівників.

На рівні операційної діяльності вирішуються такі завдання:

- обробка даних про операції, вироблених фірмою;
- створення періодичних контрольних звітів про стан справ у фірмі;
- отримання відповідей на всілякі поточні запити й оформлення їх у вигляді паперових документів або звітів.

Існує декілька особливостей, пов'язаних з обробкою даних, що відрізняють дану технологію від інших:

- виконання необхідних фірмі задач по обробці даних. Кожній фірмі наказано законом мати і зберігати відомості про свою діяльність, які можна використовувати як засіб забезпечення і підтримки контролю. Тому в будь-якій фірмі обов'язково повинна бути інформаційнасистема обробки даних і розроблена відповідна технологія;
- рішення тільки добре структурованих задач, для яких можна розробити алгоритм;
- виконання стандартних процедур обробки. Існуючі стандарти визначають типові процедури обробки даних і наказують їх дотримання організаціями усіх видів;
- виконання основного обсягу робіт в автоматичному режимі з мінімальною участю людини;
- використання деталізованих даних. Записи про діяльність фірми мають докладний характер, що допускає проведення ревізій. У процесі ревізії діяльність фірми перевіряється хронологічно від початку періоду до його кінця і від кінця до початку;
- акцент на хронологію подій;
- потреба в мінімальної допомоги при вирішенні проблем з боку спеціалістів інших рівнів.

Збір даних. У міру того як фірма виробляє продукцію або послуги, кожна її дія супроводжується відповідними записами даних.Зазвичай дії фірми, що зачіпають зовнішнє оточення, виділяються особливо як операції, вироблені фірмою.

Обробка даних. Для створення з даних, що надходять інформації, що відображає діяльність фірми, використовуються такі типові операції:

- Класифікація або угрупування. Первинні дані зазвичай мають вигляд кодів, які складаються з однієї або декількох символів. Ці коди, які виражають певні ознаки об'єктів, використовуються для ідентифікації і групування записів. Наприклад, при розрахунку заробітної плати кожна запис включає в себе код (табельний номер) працівника, код підрозділу, в якому він працює, посаду і т.п. Відповідно до цих кодами можна зробити різні угруповання;

- сортування, за допомогою якої упорядковується послідовність записів;
- обчислення, що включають арифметичні та логічні операції. Ці операції, виконувані Наляж, дають можливість отримувати нові дані;
- укрупнення або агрегування, вироблене для зменшення кількості даних і реалізоване в формі розрахунків підсумкових або середніх значень.

Зберігання даних. Багато даних на рівні операційної діяльності необхідно зберігати для подальшого використання або тут же, або на іншому рівні. Для їх зберігання створюються бази Даних.

Створення звітів (документів). В інформаційній технології обробки даних необхідно створювати документи для керівників і працівників фірми, а також для зовнішніх партнерів. При цьому документи можуть створюватися як за вимогою у зв'язку з проведеною фірмою операцією, так і періодично наприкінці кожного місяця, кварталу або року.

Існує ряд недоліків, через які неможливо використовувати отримані дані. До них відносяться недостовірність даних, низька продуктивність при нестандартних запитах, неможливість перетворити різнорідні дані в єдину інформацію.

Для різних рівнів управління організацією потрібні певні бази даних (табл. 2.1.)

Таблиця 2.1. Характеристики даних за рівнями управління

№п / п	Рівень управління	Характеристика даних
1	Операційний	Дані деталізовані. Програми націлені на обробку щоденних операцій. Зберігаються тільки поточні значення. Висока ймовірність виникнення запитів. Дані орієнтовані на використовують їх застосування

2	Корпоративний (тактичний)	Дані узагальнені. Всі значення мають позначки часу. Дані інтегровані й предметно орієнтовані
3	Рівень підрозділи (операційний і тактичний)	Зібрані дані, що мають відношення до даного підрозділу.Частково дані відносяться до примітивних, частково - до похідних
4	Індивідуальний (операційний)	Дані тимчасові. Запити нестандартні. Збір даних відбувається евристично. Операції нерутінний

Дана технологія передбачає створювати спеціальні, окремі від існуючих баз сховища даних - предметно-орієнтовані, інтегровані, некоректіруемие, залежні від часу колекції даних, призначені для підтримки прийняття рішення.

Інформаційні технології автоматизованого офісу

У міру розвитку засобів комунікації автоматизація офісних технологій зацікавила фахівців та управлінців, які побачили в ній можливість підвищити продуктивність своєї праці.

Автоматизація офісу покликана не замінити існуючу традиційну систему комунікації персоналу (з її нарадами, телефонними дзвінками та наказами), а лише доповнити її.

Інформаційна технологія автоматизованого офісу - організація та підтримка комунікаційних процесів як усередині організації, так і з зовнішнім середовищем на базі комп'ютерних мереж та інших сучасних засобів передачі та роботи з інформацією.

Офісні автоматизовані технології використовуються практично всіма службовцями організацій на різних рівнях управління. Особливо вони привабливі для групового вирішення проблем, тому що вони дозволяють підвищити продуктивність праці секретарів та інших офісних працівників, дають їм можливість справлятися зі зростаючим обсягом робіт. Проте ця перевага є другорядним у порівнянні з можливістю використання автоматизації офісу в якості інструменту для вирішення проблем, поліпшення прийнятих менеджерами рішень в результаті їх більш досконалої комунікації здатне забезпечити економічне зростання фірми.

В даний час відомо декілька десятків програмних продуктів для комп'ютерів і некомп'ютерних технічних засобів, що забезпечують технологію

автоматизації офісу: текстовий процесор, табличний процесор, електронна пошта, електронний календар, аудіопочта, комп'ютерні та телеконференції, відеотекст, зберігання зображень, а також спеціалізовані програми управлінської діяльності - ведення документів, контролю за виконанням наказів і т.д. Також широко використовуються некомп'ютерні засоби: аудіо-та відеоконференції, факсимільний зв'язок, ксерокс та інші засоби оргтехніки.

Теоретично визначаються три різні моделі офісу: інформаційна, комунікаційна та системна.

Інформаційний процес включає в себе чотири види діяльності: генерування інформації, її зберігання, поширення і сприйняття. Початок процесу - генерування інформації (інформаційних документів), закінчення - сприйняття, інтерпретація та пов'язані з цим дії. Інформація втрачає сенс, якщо немає циклу інтерпретації. Ці два процеси (генерування та інтерпретація) викликають зміну і переробку інформації.Передача в просторі і в часі не повинна змінювати змісту інформації і запропонованих інформацією дій. Генерування та інтерпретація містять творчу, слабо алгорітмізіруемую і формалізованих функцію, виконуються за участю людини, її розуму і саме тому не можуть бути повністю автоматичними.

В електронному офісі різноманітні технічні засоби забезпечують прийом і видачу трьох основних видів інформації: мови, даних, зображень у статиці і динаміці. Отже, людина може максимально використовувати всі свої способи сприйняття (слух, дотик, зір), відчуваючи тактильні і механічні дії (коли йде робота у віртуальному кіберпросторі).

Розвинені інформаційні потоки забезпечують можливість організації не тільки електронних діалогів, але і полілогу, тобто широкого обміну інформацією з кількома джерелами або партнерами.

Інтертекст - взаємодія між текстами - призводить до виникнення нових ідей та образів, оскільки зіставлення посилює інформаційну виразність тексту і оголює протиріччя. Комп'ютер як компонент інформаційних мереж стає найважливішою складовою частиною глобального полілогу, нового динамизированная способу об'єднання множинних різнорідних потоків інформації.

Інформатизація забезпечує інтеграцію професійної та інформаційної діяльності, а також докорінну зміну, професійного стилю роботи.Постановка проблеми в діалоговому режимі і її негайне інформаційне забезпечення дозволяють різко скоротити час виконання завдання, створити

зворотний зв'язок, отримати можливість оцінювати результати і змінювати умови рішення в процесі взаємодії з комп'ютером.

Сам комп'ютер в мережі стає засобом організації колективної (групової) роботи. І це ще один результат побудови електронного офісу: виникає неможливий раніше ефект групової взаємодії, у тому числі і для дистанційно розподілених партнерів.

Розвиток інформаційної технології та її апаратно-програмного забезпечення створило умови еволюційного інформаційного насичення робочих місць в офісі. Ускладнення і посилення динаміки функціонування господарських об'єктів економіки викликають необхідність отримання і обробки великих потоків інформації з безлічі різних джерел.

Інформаційні потоки (мова, зображення, текст, дані)! повинні інтегруватися на автоматизованому робочому місці в офісі. Розглянемо зазначені види інформаційних повідомлень канали передачі (зв'язку), за якими вони надходять.

Мовні повідомлення. Такі повідомлення виникають при вербальному спілкуванні співробітників як всередині офісу, так і ззовні черезтелефонну мережу. Телефон як найважливіший засіб вер бальній комунікації вдосконалюється. Його функції значно розвинулися з моменту початку експлуатації в 1878 р.

В даний час телефонна система зв'язку виконує двояку роль в офісі: вона забезпечує мовне спілкування і здійснював 'комутацію ряду технічних засобів офісу з віддаленими абонентами

Функції сучасного телефону надзвичайно різноманітні (Телефон виступає в ролі: автовідповідача; визначника номер абонента, що дзвонить (у тому числі і повідомлення про номер голосом) кошти автодозвону по зайнятому номеру в міських і міжміських мережах; блоку захисту номер телефону від його визначення зовнішніх абонентом; пристрою універсальної захисту від дзвінків небажаних абонентів. У сучасний телефон вбудовані блоки пам'яті та управління, що дозволяють розвинути функції записної книжки, калькулятора, годин, музичного супроводу, охоронної сигналізації та ін

Телефонний зв'язок колективна, тому вона порівняно дешева, однак часом буває недоступна через зайнятість ліній зв'язку і абонента іншими абонентами. Нові можливості телефонного зв'язку для подолання цієї незручності та розвитку телефонного сервісу забезпечує система радіо-пейджинг.

Можливості пейджерів у міру розвитку цієї технології зв'язку зростають. Вони:

- Забезпечують конфіденційність переданих повідомлень;

- Приймають і накопичують у пам'яті не одне, а кілька повідомлень;

- Забезпечують можливість передачі групових повідомлень відразу групі власників пейджерів і багато іншого.

Аудіоконференції. Використовують аудіосвязь для підтримки комунікацій між територіально віддаленими працівниками або підрозділами фірми. Використання аудіоконференції полегшує прийняття рішень.

Паперові документи. До них можуть бути віднесені різноманітні канали передачі паперових повідомлення та їх комбінацій (Телетайпна зв'язок, телексний зв'язок, телефаксні зв'язок та ін.) отримані паперові документи потім можуть піддаватися в офісі різній обробці, наприклад скануванню або копіюванню.

Електронна пошта дозволяє передавати й обробляти отриману кореспонденцію за допомогою комп'ютера. На практиці часто використовується для пересилки ділових документів, графіків, таблиць, фотографій і т.д.

Система інформаційного обміну телекс. Ця інформаційна система дозволяє підготувати і автоматично пересилати величезні потоки інформації різних абонентам. Система обміну телекс поступово вбирає в себе переваги телеграфу і телетайпа і покращує з. У міру розвитку системи в неї включається також можливості факсимільного зв'язку.

Інформаційна система телетекст. Телетекст - це своєрідна електронна газета або електронних бюлетень, в яких безперервно передаються сторінки тексту з газет, журналів, агентств та служб.

Інформаційна система відеотекст. Ця система розширює можливості отримання інформації та свободи вибору, а також об'єднує можливості телефону, комп'ютера і телевізора.

Автоматизація управлінської діяльності стає все більш привабливою для менеджерів усіх рівнів не тільки тому що підтримує внутрішньофірмову зв'язок персоналу, але і також тому що надає їм нові засоби комунікації із зовнішнім оточенням.

Висновок:

Застосування інформаційних технологій має великий вплив на життєздатність і конкурентоспроможність організації. підвищення ефективності підприємства завдяки використанню управлінської інформаційної системи починається з вищого рівня управління. Головний керуючий організацією повинен бачити перспективу її розвитку з урахуванням того внеску, який можуть зробити інформаційні технології.

Інформація - найважливіший інструмент бізнесу. Без інформації неможливо прийняти ключові рішення необхідні для підтримки функціонування організації. важливо розрізняти дані та інформацію. Дані розглядають як сировину, якийсь випадковий набір окремих фактів.Сьогодні дані фіксуються на наступних носіях: папері, плівці, магнітних та оптичних дисках. Зареєстровані дані можуть приймати будь-які аудіовізуальні форми, включаючи текст, зображення і звук.

І тільки тоді коли відповідні дані відібрані, організовані і належно узагальнено, виходить інформація.

Управлінська інформація - відомості про осіб, предмети, факти, події, явища і процеси, пов'язаних з управлінням. Під терміном"управлінські інформаційні системи" зазвичай розуміються системи, що містять процедури збору, зберігання, оброблення, створення і передачі інформації, необхідної для менеджерів.

Інформаційні технології - це узагальнена назва технологій застосовуваних в управлінських інформаційних системах. На сучасному підприємстві своєчасна точна інформація життєво необхідна для ефективного прийняття рішень та управління ресурсами.

У сучасній організації застосовуються такі технології:

- інформаційні технології обробки даних
- автоматизація управлінської діяльності.

Інформаційна технологія обробки даних призначена для вирішення чітко структурованих завдань, по яких є необхідні вхідні дані і відомі процедури їх обробки. Ця технологія застосовується на операційному (виконавчому) рівні. Основними компонентами інформаційної технології обробки даних є:

- Збір даних;

- Обробка даних;

- Створення звітів

Для різних рівнів управління потрібні різні бази даних. На операційному - дані деталізуються; на тактичному - дані узагальнюються; на рівні підрозділів - збираються та узагальнюються дані, що мають відношення до даного підрозділу; на індивідуальному рівні - дані мають тимчасовий характер.

Автоматизація управлінської діяльності отримала назву інформаційної технології автоматизованого офісу. Дана технологія спрямована на підтримку комунікацій як усередині організації, так і поза нею. Інформаційна технологія автоматизованого офісу передбачає наявність в організації різноманітних технічних засобів з допомогою яких забезпечується прийом і видача трьох основних видів інформації: мови, даних і зображень у їхньому теперішньому і в розвитку.

Основні інформаційні потоки інтегруються на автоматизованих робочих місцях. Основними технічними засобами автоматизації, що використовуються в інформаційних технологіях є різні модифікації телефонів, пейджерів, комп'ютерів, кошти призначені для аудіозв'язку, телефаксні зв'язок, копіювальна техніка та ін

Використання сучасних технічних засобів автоматизації дозволяє не тільки отримувати оперативну інформацію, але і на її основі приймати оперативні й стратегічні рішення.

Сучасні інформаційні технології відкривають можливість побудови інформаційно-насичених робочих місць та електронних офісів сучасно новою основою творчості, коли одиницею спілкування стає активний інформаційний екран.

На основі інформаційних технологій в організаціях створюються різноманітні інформаційні системи, призначені для управління технологічними процесами та системи адміністративно-організаційної типу для обслуговування колективу фахівців, що здійснюютьуправління підприємством.

Перелік літератури:

1. Веревченко А.П. , Горчаков В.В. Іванов І.В., Голодова О.В. Інформаційні ресурси для прийняття рішень. - К.: Ділова книга, 2004.
2. Гайфуллін Б.М., Обухів І.А. Автоматизовані системи управління підприємством. - К.: Юрінком Інтер-фейс-Прес, 2005.
3. Граубаров В.А. Інформаційні технології для менеджерів. - М.: Фінанси і статистика, 2005.
4. Ігнатьєва Д.В., Максимов М.М. Дослідження систем управління. -М.: ЮНИТИ, 2003. 157с
5. Коротке Е.М. Дослідження систем управління. М.: декла, 2003.176с

Любімов Дмитро Андрійович
Висоцький Олег Віталійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій

м. Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОБРОБКИ ДАНИХ У СИСТЕМІ УПРАВЛІННЯ

Отримання великих обсягів інформації перетворюється для фахівців з інформатики та менеджерів у серйозну проблему. Для того, щоб ідентифікувати тільки необхідну інформацію для вирішення якоїсь конкретної задачі, доводиться "перебирати" величезна кількість даних.

Про значення даної проблеми свідчить той факт, що в багатьох організаціях вводиться посада головного спеціаліста з інформації, який несе відповідальність за управління організаційними базами даних та впровадження нових інформаційних технологій. Як правило, фахівці з інформації стикаються з проблемою вибору одного з безмежного безлічі варіантів придбання апаратного та програмного забезпечення, мережевого і телекомунікаційного устаткування.

Інформаційна технологія обробки даних призначена для розв'язання добре структурованих задач, по яких є необхідні вхідні дані і відомі алгоритми та інші стандартні процедури їх опрацювання. Ця технологія застосовується на рівні операційної (виконавчої) діяльності персоналу невисокої кваліфікації з метою автоматизації деяких постійно повторюваних операцій управлінської праці.

На рівні операційної діяльності вирішуються такі завдання:

- обробка даних про операції, вироблених фірмою;
- створення періодичних контрольних звітів про стан справ у фірмі;
- отримання відповідей на всілякі поточні запити й оформлення їх у вигляді паперових документів або звітів.

Збір даних. У міру того як фірма виробляє продукцію або послуги, кожна її дія супроводжується відповідними записами даних.Зазвичай дії фірми, що зачіпають зовнішнє оточення, виділяються особливо як операції, вироблені фірмою.

Зберігання даних. Багато даних на рівні операційної діяльності необхідно зберігати для подальшого використання або тут же, або на іншому рівні. Для їх зберігання створюються бази Даних.

Існує ряд недоліків, через які неможливо використовувати отримані дані. До них відносяться недостовірність даних, низька продуктивність при нестандартних запитах, неможливість перетворити різнорідні дані в єдину інформацію.

Інформаційні технології автоматизованого офісу

У міру розвитку засобів комунікації автоматизація офісних технологій зацікавила фахівців та управлінців, які побачили в ній можливість підвищити продуктивність своєї праці.

Інформаційна технологія автоматизованого офісу - організація та підтримка комунікаційних процесів як усередині організації, так і з зовнішнім середовищем на базі комп'ютерних мереж та інших сучасних засобів передачі та роботи з інформацією.

В даний час відомо декілька десятків програмних продуктів для комп'ютерів і некомп'ютерних технічних засобів, що забезпечують технологію автоматизації офісу: текстовий процесор, табличний процесор, електронна пошта, електронний календар, аудіопочта, комп'ютерні та телеконференції, відеотекст, зберігання зображень, а також спеціалізовані програми управлінської діяльності - ведення документів, контролю за виконанням наказів і т.д.

Інформаційний процес включає в себе чотири види діяльності: генерування інформації, її зберігання, поширення і сприйняття. Початок процесу - генерування інформації (інформаційних документів), закінчення - сприйняття, інтерпретація та пов'язані з цим дії. Інформація втрачає сенс, якщо немає циклу інтерпретації. Ці два процеси (генерування та інтерпретація) викликають зміну і переробку інформації.Передача в просторі і в часі не повинна змінювати змісту інформації і запропонованих інформацією дій.

Розвинені інформаційні потоки забезпечують можливість організації не тільки електронних діалогів, але і полілогу, тобто широкого обміну інформацією з кількома джерелами або партнерами.

Інтертекст - взаємодія між текстами - призводить до виникнення нових ідей та образів, оскільки зіставлення посилює інформаційну виразність тексту і оголює протиріччя. Комп'ютер як компонент інформаційних мереж стає найважливішою складовою частиною глобального полілогу, нового динамизированная способу об'єднання множинних різнорідних потоків інформації.

Сам комп'ютер в мережі стає засобом організації колективної (групової) роботи. І це ще один результат побудови електронного офісу: виникає неможливий раніше ефект групової взаємодії, у тому числі і для дистанційно розподілених партнерів.

Інформаційні потоки (мова, зображення, текст, дані)! повинні інтегруватися на автоматизованому робочому місці в офісі. Розглянемо зазначені види інформаційних повідомлень канали передачі (зв'язку), за якими вони надходять.

Телефонний зв'язок колективна, тому вона порівняно дешева, однак часом буває недоступна через зайнятість ліній зв'язку і абонента іншими абонентами. Нові можливості телефонного зв'язку для подолання цієї незручності та розвитку телефонного сервісу забезпечує система радіо-пейджинг.

Аудіоконференції. Використовують аудіосвязь для підтримки комунікацій між територіально віддаленими працівниками або підрозділами фірми. Використання аудіоконференції полегшує прийняття рішень.
Інформаційна система телетекст. Телетекст - це своєрідна електронна газета або електронних бюлетень, в яких безперервно передаються сторінки тексту з газет, журналів, агентств та служб.

Висновок:

Застосування інформаційних технологій має великий вплив на життєздатність і конкурентоспроможність організації. підвищення ефективності підприємства завдяки використанню управлінської інформаційної системи починається з вищого рівня управління. Головний керуючий організацією повинен бачити перспективу її розвитку з урахуванням того внеску, який можуть зробити інформаційні технології.
На основі інформаційних технологій в організаціях створюються різноманітні інформаційні системи, призначені для управління технологічними процесами та системи адміністративно-організаційної типу для обслуговування колективу фахівців, що здійснюютьуправління підприємством.

Шепельський Владислав Ігорович
Державний університет телекомунікацій
Телекомунікаційні системи та мережі
Факультет Телекомунікацій
м. Київ

ТЕХНОЛОГІЯ «4G»

4thGeneration— четверте покоління пересувного (мобільного) радіозв'язку, наступник стандартів, які належать до 3G та 2G. Перший прихід поколінь відбувався при переході з аналогових (1G) до цифрових стандартів передачі на початку 1990-х (2G). Наступний крок (3G) приніс підтримку мультимедіа, передачу з розширеним спектром. Очікуваний перехід до 4G принесе All-IP із комутацією пакетів, мобільний широкосмуговий доступ із швидкостями до гігабіта за секунду при передаванні із використанням декількох несучих. Міжнародний телекомунікаційний союз до стандартів четвертого покоління відносить стандарти мобільної передачі, затверджені у специфікації ITM-Advanced у жовтні 2010 року, кандидатами у четверте покоління були визначені 6 радіоінтерфейсів, серед них варіанти LTE-Advanced(3GPPLTERelease 10) та WiMaxRelease 2 (IEEE802.16m).

Найбільш перспективними для розвитку зв'язку 4G (LTE) є частотні діапазони CDMA 800, GSM 900/1800, UMTS 2100, в яких українські оператори вже довгий час успішно розгортають свої 2G і 3G-мережі. Однак список

включає в себе також діапазони 2300-2400 МГц і 2500-2700 МГц, в яких працюють WiMAX-оператори.

Ще однією важливою перепоною, що стоїть на шляху запуску якісного 4G-зв'язку в Україні, є так зване «клаптикове» покриття.Спочатку, коли на українському телеком-ринку стався радіочастотний «бум», у регулятора не було єдиної чітко виробленої стратегії щодо того, як розподіляти частоти. Тому на сьогодні карта їх розподілу між операторами нагадує клаптикову ковдру. Так, частоти GSM 900/1800 розподілені обривками. Якщо виділити кожну наявну частоту кольором оператора, якому вона належить («Київстар» - блакитним, «МТС Україна» - червоним і lifecell - жовтим), то вийде дуже барвиста картинка, що неприпустимо для створення якісного LTE-покриття.

Вільних частот на ринку давно немає - вони нерівномірно перерозподілені між різними операторами. У одних компаній радіочастотний ресурс в надлишку, у інших же його не вистачає. Тому одним з основних завдань регулятора на даному етапі є пошук рішення, яке дозволить поставити всіх операторів в рівні умови.

Щоб очікуване LTE-покриття було максимально якісним і рівномірним, в лютому учасники ринку спільно з НКРЗІ домовилися з британською компанією Analysys Mason про проведення науково-дослідних робіт з впровадження 4G в Україні. Їх метою є пошук компромісу, який дозволив би максимально задовольнити інтереси всіх зацікавлених сторін - операторів, абонентів і держави.

Поки регулятор намагається знайти рішення, як створити основу для забезпечення якісного 4G-покриття, оператори всіляко готуються до майбутнього запуску революційної технології і тестують її. Першою в Україні новинку випробувала компанія Intellecom. На базі обладнання Ericsson вона провела публічну демонстрацію 4G-технології, досягнувши пікової швидкості завантаження 220 Мбіт/с.

«Україна, безумовно, виграє від впровадження нового стандарту мобільного зв'язку. Досвід компанії Ericsson на інших ринках свідчить, що існує тісний взаємозв'язок між розвитком мобільних технологій в країні і зростанням ВВП. Це також підтверджує недавнє дослідження GSMA: тільки в 2015 році мобільні технології принесли додаткові 3,1 мрлд дол. в світову економіку, що склало 4,2% світового ВВП » - розповів Салман Атік - керівник напряму мобільних мереж компанії Ericsson в регіоні Північної Європи і Центральної Азії.

4G-технологія передбачає не просто більш швидку швидкість інтернет-з'єднання. Вона є своєрідною базою для реалізації нових комплексних

соціальних проектів. Йдеться, зокрема, про створення «розумних» міст, «розумного» транспорту, «розумного» сільського господарства. Такі проекти залежать від якості та швидкості передачі даних і не можуть бути повністю реалізовані на швидкостях мережі 3G.

Хоч і близький довгоочікуваний момент запуску 4G, Україна як і раніше відстає від цивілізованих країн за темпами впровадження нових технологій. У той час, коли наша країна захоплено очікує запуску зв'язку четвертого покоління, Європа вже вивчає перспективи впровадження 5G і чекає того ж від України.

ЛІТЕРАТУРА
1. Інформаційне агентство УНІАН «4G-зв'язок в Україні»,http://economics.unian.net/
2. А.П. Бондарчук, Г.С. Срочинська, М.Г. Твердохліб-«Основи інфокомунікаційних технологій», 2015р.
3. «ВІКІПЕДІЯ.Вільна енциклопедія»: https://uk.wikipedia.org

Журавель Катерина Ігорівна
ержавний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

АЛГОРИТМ І ЙОГО ЗНАЧЕННЯ В ІНФОРМАТИЦІ

Як комп'ютери вирішують задачі? Коли ми купуємо щось в Інтернеті, як забезпечується захист кредитної картки від перехвату зловмисників? Як GPS в лічені секунди знаходить найкоротший шлях? Що таке алгоритми і яка їхня роль у житті людей, а особливо в бутті програмістів? Перший крок до розуміння важливості вивчення і знання алгоритмів це дати точне визначення того, що розуміється під алгоритмом. Поняття алгоритму в інформатиці являється фундаментальним, тобто таким, яке не визначається через інші, ще більш прості поняття. Простими словами алгоритм – це набір кроків, які визначають яким чином буде виконана задача.Завдяки здатності фіксувати і висловлювати свій розум (або, щонайменше, розумну поведінку) за допомогою алгоритмів, ми здатні створювати обчислювальні машини, які виконують корисні завдання.

Навіщо ж програмістам, які не вирішують складних завдань, знати алгоритми? А для того, щоб бути кваліфікованим фахівцем і ефективно використовувати доступні інструменти, включаючи мову, на якій пишуть, так як алгоритми служать для стандартизації описів будь-яких процесів. Без них були б неможливі будь-які види обчислень, а рішення будь-якої проблеми починалося

б з «нуля» – навіть якщо вона була вирішена безліч разів. Розвиваючи глибоке розуміння широкого діапазону алгоритмів, ви зможете вибрати вірну послідовність дій і застосувати її для вирішення завдання.

Можуть запитати - до чого всі ці розмови? Хіба сучасні комп'ютери не складається два числа за один крок? Є дві відповіді. По-перше, дійсно, за один крок можна скласти два числа, які поміщаються вмашинне слово (зазвичай 32 або 64 біта). Однак, як ми побачимо, частонеобхідно працювати з набагато довшими числами, і їх волею-неволеюдоводиться розбивати на частини. По-друге, хоча додавання машинних сліввиробляється однією командою, всередині процесора ця команда складається збагатьох операцій з окремими бітам. І число таких бітових операцій суттєво, оскільки від нього залежить кількість функціональних елементів (транзисторів, проводів і т. д.), необхідних для реалізації алгоритму «в залізі».Алгоритми - настільки ж важлива начинка, як і всі залізяки. Іншими словами інформатика без алгоритмів – це як вища математика без таблиці множення.
Глибоке знання можливо і не потрібне, але загальне розуміння і знання що робить конкретний алгоритм, для чого можна використовувати конкретну структуру даних - потрібні. А якщо доведеться реалізувати щось конкретне для своїх цілей, то завжди можна подивитися літературу для деталей.

Список літератури:
1. https://habrahabr.ru/post/279453/
2.http://itandlife.ru/science/computer-science/rol-algoritmov-v-informacionnyx-texnologiyax/

Буренко Андрій
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет телекомунікацій
м. Київ

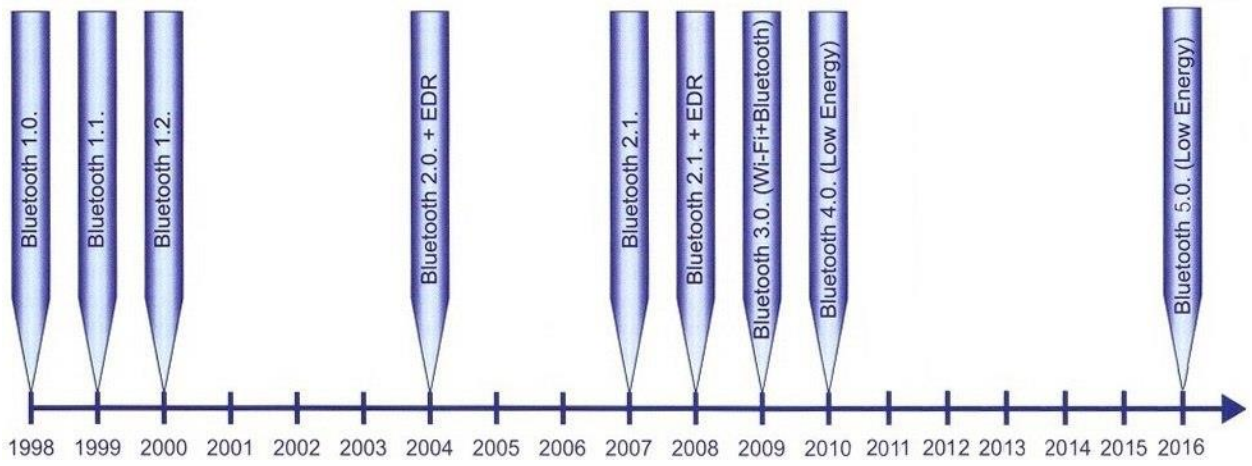
ТЕХНОЛОГІЯ BLUETOOTH 5

Технологія Bluetooth є твердо усталеним комунікаційним стандартом для бездротового зв'язку на малих відстанях, поєднуючи пристрої за допомогою однієї універсальної радіолінії з малим радіусом дії. Розгортання цієї технології базується на використанні мережі WPAN, стандарту, розробленого робочою групою IEEE 802.15

Для роботи радіоінтерфейсуBluetooth використовується так званий нижній (2,45 ГГц) діапазон ISM (Industrial, Scientific, Medical), призначений для роботи промислових, наукових і медичних приладів.У Bluetooth застосовується метод розширення спектра зі стрибкоподібною перебудовою частоти (англ.

FrequencyHoppingSpreadSpectrum, FHSS).Коротко це можна пояснити так: передавач розбиває дані на пакети і передає їх за псевдовипадковим алгоритмом стрибкоподібної перебудови частоти(1600 разів в секунду), або шаблоном (pattern), складеному з 79 підчастот. «Зрозуміти» один одного можуть тільки ті пристрої, які налаштовані на один і той самий шаблон передачі — для сторонніх приладів передана інформація буде звичайним шумом. Інтерфейс Bluetooth дає змогу передавати як голос (зі швидкістю 64 Кбіт/с), так і дані. Для передачі даних можуть бути використані асиметричний (721 Кбіт/с в одному напрямку і 57,6 Кбіт/с в іншому) та симетричний (432,6 Кбіт/с в обох напрямках) методи. Працюючи на частоті 2.4 ГГц, прийомопередавач (Bluetooth-chip) дає змогу встановлювати зв'язок у межах 10 або 100 метрів. Різниця у відстані, безумовно, велика, однак з'єднання в межах 10 метрів дає змогу зберегти низьке енергоспоживання, компактний розмір і досить невисоку вартість компонентів.

На сьогодні існує 9 основних специфікацій технології Bluetooth, хронологію їх випуску наведено на схемі нижче:



Докладніше розглянемо саме останню - Bluetooth 5.

17 червня 2016 року консорціум BluetoothSpecialInterestGroup (Bluetooth SIG) представила наступну версію стандарту Bluetooth - 5. Її появу на комерційному ринку заплановано на кінець 2016 або початок 2017 року.

Bluetooth 5 запропонує вчетверо більший радіус дії, вдвічі більшу швидкість передачі даних і у вісім разів збільшену ємність повідомлення безконтактної радіопередачі. Це перше значне оновлення стандарту починаючи з 2009 року, коли ефір побачив Bluetooth 4.

Завдяки збільшенню ємності радіоповідомлень, буде можлива передача складнішої, інтелектуальної інформації. Це призведе до зміни способу передачі інформації Bluetooth-пристроями. Модель створення пари піде в минуле. На її місце прийде так зване безконтактне з'єднання.

Для з'єднань з низьким енергоспоживанням за технологією BluetoothLowEnergy (Bluetooth LE) стандарт Bluetooth 5 значно збільшить радіус дії і швидкість, при цьому ємність переданих повідомлень «без встановлення з'єднання» виросте на 800%.

Подивившись поточні характеристики Bluetooth LE легко з'ясувати що мова йде про діапазон до 200 метрів і швидкість передачі до 4-12 Мбіт/с. Все це без підвищення енергоспоживання, в порівнянні з поточним стандартом.

Крім того, ці нововведення дуже позитивно вплинуть на сферу інтернету речей (IoT). Впровадження нового покоління зв'язку призведе до зростання числа IoT-пристроїв з підтримкою Bluetooth і дозволить зробити реальністю більш просунуті розумні будинки.

«*Bluetooth 5 змінить образ взаємодії людей з IoT, зробивши його більш простим. Збільшення радіусу дії зв'язку дозволить підключати до інтернету речей більше пристроїв. При цьому вони будуть швидше обмінюватися даними і отримувати оновлення ПЗ. Більший обсяг переданих даних дозволить зробити значно зручнішим використання різного роду маячків і інших сервісів, не пов'язаних з мобільним*», - заявив виконавчий директор Bluetooth SIG Марк Пауел.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Олифер В.Г., Олифер Н.А.- Компьютерные сети. Принципы,технологии, протоколы (4-е издание), 2010 - 943с.
2. А.П. Бондарчук, Г.С. Срочинська, М.Г. Твердохліб-«Основи інфокомунікаційних технологій», 2015 – 76с.
3. «ВІКІПЕДІЯ.Вільна енциклопедія»: https://uk.wikipedia.org
4. IT-портал «TECHLIFE» : http://rus.delfi.lv/techlife/
5. Інтернет журнал «NavkoloNas» : http://navkolonas.com/

Марчук Анна Николаевна
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

FREENET - ИНТЕРНЕТ БЕЗ ЦЕНЗУРЫ

Я волнуюсь о своем ребенке и интернете все время. И хотя моя дочь сейчас слишком мала, чтобы войти в сеть, я переживаю о том, что лет через 10-15 она придет ко мне и скажет: "Папа где ты был, когда они приняли закон о цензуре прессы. Майк Годвин. Фонд электронных рубежей.

На протяжении истории человек всегда нуждался в свободе слова, и хотя право на свободу слова официально признаны, думаю, в каждом государстве, на самом же деле это может быть не всегда, и не для всех правдой. Вот одна из причин по которой была создана сеть под названием Freenet.

Freenet - анонимная децентрализованная, одноранговая сеть, предназначенная для распределенного хранения данных без возможности их цензуры, созданная с целью предоставить пользователям электронную свободу слова путём обеспечения их строгой анонимности. Freenet работает на основе объединения в общий фонд предоставленной пользователями своей полосы пропускания (скорости) и дискового пространства своих компьютеров для публикации, или получения из Freenet разного рода информации. Freenet использует разновидность маршрутизации по ключам. То есть для того, чтобы вам получить ваш загруженный файл в сеть Freenet вам нужно указать специальный ключ, который подтверждает, что файл принадлежит вам.

Мир тесен
Freenet строится на принципе графов “малого мира”. Этот граф имеет такую особенность: если взять две произвольные вершины a и b, то они с большой вероятностью не являются смежными, однако одна достижима из другой посредством небольшого количества переходов через другие вершины.

Чтобы было более понятнее Freenet передает информацию, системой интернет, он не имеет выделенного канала связи, но работает параллельно (отдельно) от всего интернета. То есть из freenet вы не сможете получить доступ к google, vk и instagram. Кроме того вы сами не сможете получить доступ к Freenet, не используя веб “костылей” Он работает с того же браузера, которым вы пользуетесь.

Однора́нговая сеть (англ. peer-to-peer, P2P равный к равному) сеть это компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют центральные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.
Примерами p2p сетей могут служить такие известные продукты, как bittorrent, или
bitcoin.
Суть технологии заключается в том, что хотя ты и используешь сеть ты отдаешь часть своих ресурсов (обычно незначительную часть для лучшего функционирования всей сети). Ты всем и все тебе.

Кто стоит за Freenet?

Идея Freenet выросла из идеи анонимного распределенного хранилища, опубликованной в докторской работе профессора Яна Кларка в Университете Эдинбурга, Шотландия. С тех пор многие другие люди внесли свой вклад в это дело.
Freenet находится в стадии разработки с 2000 года. Хотя версия 1.0 ещё не выпущена, текущие версии достаточно стабильны для практического использования.

Для чего нужен Freenet?
Существует множество других анонимных сетей, зачем еще одна? Эта рассчитана для предоставления свободы слова, строгой анонимности, общения, невозможности удаления материалов третьими лицами и другие.
Из-за того, что сеть децентрализована,у нее нет серверов, серверами выступают сами клиенты, она не может быть уничтожена, даже при самом жестком диктаторском режиме, поскольку будет существовать даже при существовании двух компьютеров. Система построена таким образом, что не зависит от числа компьютеров в ее сети, но чем больше компьютеров в ней участвуют, тем больше и скорость загрузки / передачи.
Freenet является распределенным хранилищем так, как контент загруженный в Freenet, будет оставаться на Freenet, до тех пор, пока он востребован, не опасаясь цензуры, или отказа в обслуживании, и без необходимости запускать свой собственный веб-сервер, сохраняя его онлайн постоянно.

Еще одна большая разница в том, что Freenet имеет режим "даркнета", или “малого мира”, где ваш узел Freenet (программное обеспечение на вашем компьютере) подключается только к Freenet узлам принадлежащих вашими друзьями, то есть людей, которых вы знаете и доверяете.
Тем не менее, большинство людей в настоящее время используют Freenet в режиме "OpenNet" (то есть, подключение автоматически к тому, кто в сети, а не только к своим друзьям).

Основными особенностями этой сети есть
Тайная идентичность
Для отсутствия спама в анонимной сети предусмотрен плагин под названием доверительная сеть (Web Of Trust). Он поможет найти ваших знакомых и доверенных личностей в этой сети. Для того, чтобы стать довереной идентичностью нужно разгадать загадку созданную оппонентом, тем самым подтвердив свою доверенность.
Децентрализованная
Информация может быть загружена в Freenet, не будучи загружена на сервер.
Адаптивное кэширование
Многие современные системы помогают поделиться информацией в сети. Freenet адаптивно кэширует информацию по мере необходимости ее спроса, Это позволяет Freenet работать на "расширение масштабов" гораздо быстрее,

чем большинство решений для анонимного обмена файлами, а также улучшает балансировку нагрузки.
Высокая безопасность
Freenet уже давно-поддерживает концепцию "Content Hash ключи" , которые гарантируют целостность полученных данных. Freenet также поддерживает "Ключи цифровой подписи" , которые позволяют пометить файлы собственной цифровую подпись. Цифровая подпись гарантирует неизменяемость передаваемого контента.
Прямое исправление ошибок
Даже при неполном получении файла Freenet может использовать метод “прямого исправления ошибок” для того, чтобы восстановить недостающие части. Freenet также поддерживает "исцеление", который включает в себя реконструкцию и реинтеграции недостающих компонентов файла.

Недостатки прочих сетевых систем
Существует две основных проблемы в проектировании анонимных сетей. Это конфиденциальность и доступность. Если делать упор на конфиденциальность, то продвинутые системы защиты требуют определенных технических навыков. Кроме того, они могут ограничивать вас в скорости подключения, использовании распространенных протоколов, что весьма неудобно, а иногда и не уместно. Все зависит от того для чего вы используете анонимные сети. По этим причинам они могут быть недоступны для рядовых пользователей. Freenet, хотя и имеет свои минусы он нацелен как для производителей, так и для потребителей информации. Он достаточно устойчив, чтобы не дать третьим лицам запретить доступ к информации.

Технические детали
Любые данные в freenet имеют название в форме ключа
Узлы в сети посылают запросы для поиска нужных файлов.
Каждый узел имеет свое собственное локальное хранилище, доступное сети для чтения и записи.
Динамическая таблица маршрутизации, так сказать маршрутизатор сети содержит адреса других узлов и ключи, файлов находящихся на них.
Пользователям предоставляются возможность расширения локального хранилища
Запросы по ключам передаются от узла к узлу. Это значит, что если файл был передан в другой узел, запрос вначале передается на прошлый, пока не достигнет цели.
Каждый узел знает только своих двоих соседей
Ни один узел не имеет привилегию над любым другим узлом.

Keyword-Signed Keys
Ключевое слово подписания ключей (KSK)

Ключевое слово позволяет сохранить названные страницы в Freenet. Но такая система не защищена от угона имени. Например, каждый человек мог бы получить одинаковые ключи-имена. Для таких целей существует система предотвращения столкновения имен. Она контролирует, чтобы прошлые ключи файлов и имена страниц не перезаписывались новыми. Адресном KSK выглядит следующим образом:

Пользователь вычисляет двоичный ключ для файла и отправляет сообщение на узел, определяющий повторялось, ли это значение. Если подобно имя-ключ найдено система возвращает его назад до тех пор, пока не будет найден уникальный ключ.

Узел хранения
Когда новый файл прибывает, к узлу, хранилище, которого превышает размер указанный при создании этого хранилища, прошлые файлы выселяют в порядке от старого к новому, пока не освободится место
Преимущество: Этот метод позволяет естественно удаляться устаревшим документам.

Минусы
Использование "анонимного" Интернета не всегда оправдано: Подключение к Facebook через Tor не мешает Facebook знать о вас практически все, подключение к сети не используя HTTPS протокол, может означать, что кто то может украсть ваш пароль учетной записи.
Скорость в сети Freenet низкая, из-за протоколов и программ нацеленных на сохранение анонимности.
Freenet отдельная сеть, которая работает по-другому, потому что в сети нет центральных серверов. Поэтому Freenet не использует Javascript, сценариев на стороне сервера и т.д. Все функционирует в режиме распределенной сети. Если нет центрального сервера, значит его невозможно закрыть.

Freenet является попыткой устранить возможность для любой группы лиц навязывать свои убеждения и ценности другим. Многие государства осуществляют цензуру коммуникаций в тех, или иных пределах. При этом можно выделить одно общее свойство: некоторое лицо решает, какую информацию запретить, а какую допустить. В то же время то, что может быть приемлемо для одной группы людей, может рассматриваться как оскорбительное или даже опасное для другой. По существу, основным замыслом Freenet является то, что никому не позволено решать, что приемлемо. В сети поощряется терпимость к ценностям других, а, в случае отсутствия последней, пользователей просят закрыть глаза на содержание, которое противоречит их взглядам.

Для просмотра и обмена данными в сети Freenet созданы такие продукты как:

Free sites это популярный способ использования Freenet. Free sites это статические веб-сайты-каталоги, которые находятся внутри сети Freenet и доступны только через сеть Freenet. Самый простой способ, чтобы начать исследовать мир Freenet.
FMS (Freenet Message System) является внешним приложением, самым популярным средством связи на форумах, но не официальным, поскольку не входит в официальный релиз сети и написан на языке C++, который не такой безопасный, как Java.
Sone - это плагин, который обеспечивает связь в стиле социальной-сети (по образцу Facebook) в сети Freenet. Не является официальнім приложением freenet.
Freemail это плагин , который обеспечивает связь по электронной почте по сети Freenet.
Frost -является внешним приложением, которое предоставляет систему отправки сообщений и общий доступ к файлам с помощью сети Freenet. Он имеет простой в использовании интерфейс, чтобы комфортно управлять своими вставками и загрузки и общаться с другими людьми, используя сильное шифрование. Проект был начат в 2001 году и находится под постоянным развитием с тех пор.
Freetalk это плагин, который предлагает форумный стиль общения в Freenet.
Анонимная публикация сайтов, не сохраняемых на сервере. jSite представляет собой графическое приложение, которое можно использовать для создания, вставки и управлять своими собственными сайтами в freenet.
В сети freenet и для взаимодействия с ней, возможно написание собственных приложений. freenet client protocol инструмент созданный для того, чтобы иметь возможность:
Загружать в и выгружать из данные Freenet, запрашивать статус сети

Все пользователи Freenet вносят часть своего места на жестком диске для хранения зашифрованных частей файлов пользователей сети. Они хранятся в каталоге- хранилище данных Freenet.
В отличие от других подобных равноправных сетей, где пользователи имеют малый, или не имеют вообще никакого контроля над тем, что хранится в хранилище данных. В таких сетях файлы хранятся, или удаляются в зависимости от того, насколько они популярны. Это позволяет Freenet быть цензуро устойчивой. Там нет функции "удалить файл".
Расшифровать зашифрованные файлы, хранимые на жестком диске компьютера сложно, но не невозможно.
Freenet предполагает использование памяти вашего компьютера, в зависимости от того сколько вы сами определите. Чем больше памяти вы определите под использование freenet, тем больше он будет потреблять оперативной памяти. Но это дает вам приоритет скорости при использовании freenet.
Если авторы являются анонимными, как вы можете доверять информации?

Криптографически подписание информации позволяет людям доказать авторство, этот метод часто используется для проверки подлинности авторства писем. Кроме того, вы можете подписать информацию, оставаясь при этом анонимным, таким образом имея анонимный персону. Вы можете доказать, что вы написали различные части информации о Freenet, не раскрывая свою личность. Таким образом, вы можете создать анонимную репутацию надежности.

Логотип
Зайка в прыжке это логотип freenet. Он символизирует прыжок через цензуру.

Практическое использование
Для того, чтобы начать использовать Freenet вам достаточно скачать клиент, при необходимости закачать java пакет, что делается автоматически, запустить и использовать. Клиент Freenet использует ваш браузер в режиме инкогнито.

Морозов Костянтин Костянтинович
ДержавнийУніверситетТелекомунікацій
Факультет Телекомунікацій
м. Київ

РОБОТА У СИСТЕМАХ ВІЗУАЛЬНОГО ПРОГРАМУВАННЯ ДО ВИВЧЕННЯ МОВ ВИСОКОГО РІВНЯ І ОБ'ЄКТНО-ОРІЄНТОВНОГО ПРОГРАМУВАННЯ

Програмування займає одну із значних ніш в сучасному світі. Це не просто спосіб змусити працювати «залізяки», але й спосіб поставити себе на шлях розвитку своїх здібностей.

Основи програмування в наші дні викладають ще в школі в процесі вивчення інформатики. Звичайно, це далеко не ті знання, які надаютькурси С ++ для початківців програмістів, але з їх допомогою дитина вже починає розуміти, що це таке. Зокрема в сучасних школах на сьогодні день дітям пропонують засвоїти візуальний тип програмування.

Варто відзначити, що насправді візуальне програмування, хоча і викладається в школах, воно також є фундаментом для розуміння у наступному мов високогорівня. Складність програмування в основному полягає в серйозній розумовій віддачі, яку воно потребує та способі мислення. Візуальний же спосіб програмування зможе краще допомогти розібратись з логікою роботи інших мов.

Мови високого рівня відрізняються від звичайних тим, що вона розроблена для простоти використання програмістами і використовує абстракції, що на машинному коді, чи на низькорівневих мовах програмування виглядали доволі довгими та незрозумілими.

Об'єктно-орієнтоване програмування – методологія програмування, заснована на представленні програми у вигляді сукупності об'єктів, кожен з яких є екземпляром певного класу, а класи утворюють ієрархію спадкування.

Візуальне програмування – спосіб створення програми для комп'ютера шляхом маніпулювання графічними об'єктами замість написанняїї тексту. Візуальне програмування часто представляють як наступний етап розвитку текстових мов програмування. Наочним прикладом може служити утиліта Візуальний Pascal або Microsoft Visual Studio, де редагуються графічні об'єкти і одночасно відображається відповідний текст програми. Останнім часом візуальному програмуванню стали приділяти більше уваги - в зв'язку з розвитком мобільних сенсорних пристроїв (КПК, планшети).

Система візуальної розробки Алгоритм має риси притаманні більшості мовам програмування. При навичках роботи в данному середовищі перейти до розробки в середовищі Паскаль буде легко, та не складе труднощів.

Хоча система алгоритм передбачає введення коду, сама ідея візуального програмування схожа на об’єктноорієнтовну мову саме блоками - об’єктами.

Крім блокових систем візуального програмування, можна виділити ще пазлову систему. До таких належать Scratch та Blockly.

Сьогодні все більше людей різних спеціальностей мають справу з програмуванням і для того, аби створити його для усіх, розробники продуктів програмування, і не тільки, використовують системи візуального програмування, як альтернативний, або основний інструмент. Як приклад ігровий двигун Unreal Engine використовує систему візуального програмування Blueprint, за допомогою якої можливо як створити систему інвентарю персонажа, так і згенерувати цілий рівень.

Хоча наразі методи візуального програмування не мають такої популярності, як раніше, проте без сумніву їх вивчення корисне для зрозуміння логіки кодування. Проте не слід також вважати, що системи візуального програмування створені лише для першачків програмування.

Одне з кращих визначень візуального програмування можна зустріти в роботах Маргарет Барнет (Margaret Burnett) – воно настільки вдало, що його визнали гідним внесення в енциклопедичний словник електрики і електроніки. Отже, «візуальне програмування – це програмування, в якому для передачі семантики (система правил тлумачення окремих мовних конструкцій. Семантика визначає смислове значення пропозицій алгоритмічної мови) використовується більш

ніж один вимір. Як приклади таких додаткових вимірів можна привести застосування багатовимірних об'єктів, просторових або тимчасових відносин для специфікації семантики відносини до-після ». Традиційна (мовна) техніка програмування з семантичної точки зору одномірна, тому як семантика програми визначається «лінією» - рядком тексту, що містить власне програму (Барнет згадує про можливе «другому вимірі» - коментарі та документації, які тільки уточнюють, пояснюють, але ніяк не визначають семантику). Багато різновидів поширених інструментальних засобів в якійсь мірі відповідають наведеним визначенням: так, редактори діаграм і просто графічні редактори, що дозволяють вільно, «від руки» малювати електронним пером, можуть бути (і часто бувають) основою і систем візуального програмування. Останні, до слова, здатні грати роль транслятора з «багатовимірногомови» в «одновимірний».

Література:

6. Блог http://mybuzines.ru/?p=20281
7. https://tproger.ru/translations/c-importance-for-new-developers/
8. Блог http://eax.me/first-programming-language/
9. http://itc.ua/articles/vizualnoe_programmirovanie_20466/
10. https://habrahabr.ru/post/249965/

Олейник Наталья Александровна
Государственныйуниверситеттелекоммуникаций
Факультет Телекоммуникаций
г. Киев

ВАЖНОСТЬ ИЗУЧЕНИЯ ПРЕДМЕТА ИНФОРМАТИКА НА ПЕРВОМ КУРСЕ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Информатика – это область человеческой деятельности, связанная с ***процессами*** преобразования информации с помощью компьютеров.

Основной задачей информатики как науки - это систематизация приемов и методов работы с аппаратными и программными средствами вычислительной техники. Цель систематизации состоит в том, чтобы выделять, внедрять и развивать передовые, более эффективные технологии автоматизации этапов работы с данными, а также методически обеспечивать новые технологические исследования.

В ходе современной научно-технической революции общество вступило в полосу всеохватывающей автоматизации.

Цель исследования состоит в том, чтобы определить важность изучения информатики на первом курсе ВУЗа

Объектом исследования является предмет информатики
Предмет исследования- достижения в сфере информатики
Задание исследования предусматривает:

- определение важности предмета информатика
- важность изучения алгоритмов
- область применение полученных навыков и знаний
- пример решения простейшей задачи и ее практическое применение

Важность изучения информатики состоит в том, что люди, живя в мире технологий, не могут обойтись без гаджетов и прочей вычислительной техники. Наш мир постоянно развивается и становится всё более сложным, информатика нужна для восприятия всей этой информации.

Одними из самых важных достижений в сфере информатики являются:

- беспроводные сети(Wi-Fi)

Преимущества: высокая скорость и легкость в создании сети; небольшое количество проводов на рабочем месте; сравнительно низкая стоимость.
Недостатки: чем больше подключено устройств к точке доступа, тем меньше будет скорость передачи данных; риск взлома по причиненизкойнадежности.

- новые устройства и программы

А именно: уменьшение размеров компьютера, разработка новых ОС(Windows, Linux), улучшение офисов(MicrosoftOffice 97/2000), появление программ-переводчиков(Система Сократ и ПРОМТ), создание антивирусов(AVP)

- система дистанционного образования

Преимущества: мобильность, доступность, свобода и гибкость графика изучения, индивидуальная скорость обучения.
Недостатки: отсутствие общения между учениками и преподавателями, недостаток практических и лабораторных занятий, возможность изложения информации только в письменном виде, отсутствие контроля над учениками.

Информатика предоставляет возможности для решения самых разнообразных теоретических и практических задач. Применение вычислительной техники в фундаментальной науке позволяет быстро и эффективно находить решения многих научных проблем. Информационные технологии широко используются в технике. Важным этапом развития общества стала информатизация, которая вывела коммуникации на новый уровень, сделав возможными такие вещи, как удалённая работа и обучение, позволив огромному числу людей общаться, почти мгновенно узнавать новости по всему миру.

Основными задачами информатики являются:

- исследования информационных процессов любого происхождения
- решение многих научных проблем
- внедрение техники в различные сферы жизни человека
- поиск новейших разработок по переработке информации

СРАВНЕНИЕ ИЗУЧЕНИЯ В ДРУГИХ ВУЗАХ (КПИ, НУ ШЕВЧЕНКО,)

КПИ: Разработка и эксплуатация программных продуктов и технических средств компьютерных и компьютеризированных систем и сетей, внедрение современных информационных технологий общего и целевого назначения для различных отраслей науки и промышленности. Они способны создавать и эксплуатировать компьютерные и компьютеризированные системы обработки информации и управления организационных, технических и организационно-технических объектов.

НУ Шевченко:

Изучение программного обеспечения интеллектуальных систем; интеллектуальные информационные технологии; информационные технологии и системы; технологии программирования; интеллектуальная обработка информации и знаний; системный анализ и принятие решений; стохастический анализ систем; исследования операций; моделирование и оптимизация систем; вычислительная математика.

МТИ: вычислительные машины, комплексы, системы и сети; автоматизированные системы обработки информации и управления; системы автоматизированного проектирования; программное обеспечение средств вычислительной техники и автоматизированных систем, математическое, информационное, техническое, эргономическое, организационное и правовое обеспечение перечисленных систем.

МИФИ: изучение языков программирования, алгоритмов и структур данных; программных и аппаратных средств информатики и математического программного обеспечения; математической логики и дискретной математики; программирование на C++ и прикладное программное обеспечение; операционные системы, и системное программное обеспечение; телекоммуникации, компьютерные сети и web-технологии; разработка и управление базами данных, языки запросов; элементы функционального анализа, метрология и стандартизация; теория вероятностей, математическая

статистика, прикладная статистика; численные методы, решение уравнений математической физики и оптимизация; математическое и имитационное моделирование; исследование операций, теория игр и динамическое программирование; теория случайных процессов и массовое обслуживание; теория управления, цифровое и оптимальное управление, нелинейные системы; компьютерная графика, обработка сигналов и изображений, распознавание образов; базы знаний, экспертные системы и поддержка принятия решений; искусственный интеллект и технологии обучения.

ГУТ: изучается инженерная и компьютерная графика, информационные системы и технологии, компьютерная графика и моделирование, компьютерная графика, компьютерные сети и телекоммуникации, объектно-ориентированный анализ и программирование, вычислительная техника и микропроцессоры, вычислительная техника и программирование, организация баз данных, основы информатики, программирование, создание и обработка баз данных ПЭВМ, техническая графика, цифровая обработка сигналов, компьютерная графика и мультимедиа, проектирование интеллектуальных систем, цифровые системы телевидения и радиовещания, исследование и проектирование интеллектуальных систем, технологии программирования.

Таким образом, следует сделать вывод, что в КПИ суть предмета информатика- внедрение в разные сферы человеческой деятельности компьютеров и вычислительной техники в целом.
Основной областью изучения на факультете информационных технологий в НУ Шевченко являются интеллектуальные системы.
Если сравнивать МТИ и МИФИ, то в первом акцент делается на автоматизации, во втором- на математическом ПО.
В ГУТетелекоммуникационные и информационные сети тесно связаны между собой, что нельзя оставить без должного внимания, т.к. сфера деятельности университета применима во всех областях современного общества.

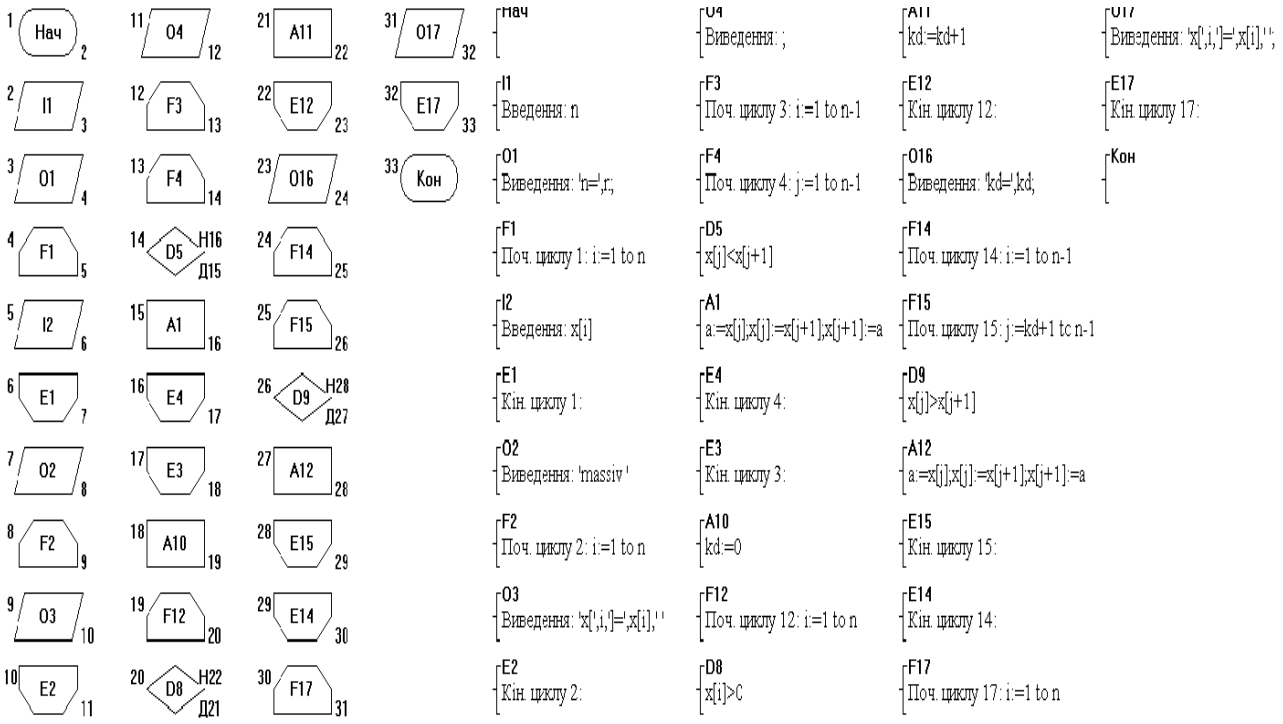
Алгоритм- одна из простейших на первый взгляд программ для решение задач.

Умение пользоваться программой Алгоритм необходимо для дальнейшего изучения программирования. В основе программирования в Алгоритме лежат принципы классического программирования в дисковой операционной системе. Достижение результатов в программировании возможно лишь при постоянной практике и решении конкретных прикладных задач.

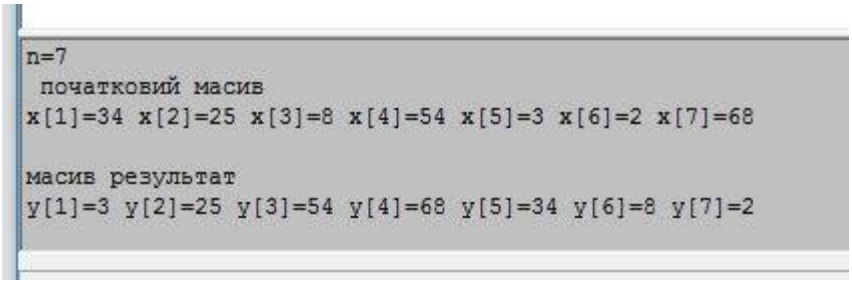
Алгоритм применяется для решения классических задач по информатике. Проектирование в алгоритме можно считать универсальным средством решения задач. Их применение не ограничивается только традиционными задачами вычислительной техники и математики. Все больше программ и приложений выходят за рамки традиционной области их применения. Будем надеяться, что это тенденция сохранится и в будущем.
Основной целью программы в университетах является выработка у студентов навыков решения поставленных задач. Курс изучения программы Алгоритм вырабатывает специфические навыки решения задач.

Рассмотрим простую задачу.

Дано: одномерный массив. Нужно сделать так, чтобы по центру находился самый большой элемент массива, а по бокам- остальные элементы в порядке их спадания.



Для того, чтобы найти максимальный элемент массива, нам нужно было сравнить все элементы массива между собой. Далее, чтобы рассортировать оставшиеся элементы в порядке их спадания, нам нужно было их так же сравнить, как и в первой части задачи, а далее ввести цикл с параметром(j:= 1 to n-1) и вывести массив.



В процессе решения этой задачи студенты приобретают навыки ввода- вывода массива, учатся использованию циклов с параметрами, а так же поиску специфических методов решения поставленных задач.

Литература

[1, https://www.it-lines.ru/blogs/network/preimushhestva-i-nedostatki-provodnyx-i-besprovodnyx-setej];
[2, http://ref.by/refs/67/32138/1.html];
[3, http://www.wikiznanie.ru/wikipedia/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0];
[4, http://imcs.dvfu.ru/lib/eastprog/informatics.html];
[5, http://kpi.ua/ru/node/7058];
[6, http://www.univ.kiev.ua/ru/dep/kiber/];
[7, http://www.bakalavr-magistr.ru/course/Vyichislitelnyie-mashinyi-kompleksyi-sistemyi-i-seti-2-vyisshee];
[8, https://mephi.ru/about/faculty/Faculty-of-Cybernetics-and-Information-Security/chairs/chair17/index.php];
[9, http://www.dut.edu.ua/ru/];
[10, Левитин А.В. Алгоритмы. Введение в разработку и анализ: Пер. с англ.-М.: Издательский дом «Вильямс», 2006.- с.14-16.];
[11, http://www.yaklass.ru/materiali?mode=lsntheme&themeid=203].

Вєдєрнікова Дениса
Заремовського Миколи
Державний Університет Телекомунікацій
факультет телекомунікацій
м. Київ

ПРОБЛЕМИ І ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Сучасні інформаційні технології.

Сучасний період розвитку цивілізованого суспільства характеризує процес інформатизації.

Інформатизація суспільства - це глобальний соціальний процес, особливість якого полягає в тому, що домінуючим видом діяльності в сфері суспільного виробництва є збір, накопичення, продукування, обробка, зберігання, передача

та використання інформації, здійснювані на основі сучасних засобів мікропроцесорної та обчислювальної техніки, а також на базі різноманітних засобів інформаційного обміну.
Інформатизація суспільства забезпечує:

- Активне використання постійно розширюючого інтелектуального потенціалу суспільства, сконцентрованого в друкованому фонді, і науковій, виробничої та інших видах діяльності його членів;
- Інтеграцію інформаційних технологій в наукових та виробничих видах діяльності, ініціюючій розвиток всіх сфер суспільного виробництва, інтелектуалізацію трудової діяльності;
- Високий рівень інформаційного обслуговування, доступність будь-якого члена суспільства до джерел достовірної інформації, візуалізацію представленої інформації, суттєвість використовуваних даних.

Застосування відкритих інформаційних систем, розрахованих на використання всього масиву інформації, доступної в даний момент суспільству в певній його сфері, дозволяє удосконалити механізми управління суспільним устроєм, сприяє гуманізації і демократизації суспільства, підвищує рівень добробуту його членів. Процеси, що відбуваються у зв'язку з інформатизацією суспільства, сприяють не тільки прискоренню науково-технічного прогресу, інтелектуалізації всіх видів людської діяльності, а й створенню якісно нового інформаційного середовища соціуму, що забезпечує розвиток творчого потенціалу індивіда.
Один з напрямків процесу інформатизації сучасного суспільства є інформатизація освіти - процес забезпечення сфери освіти методологією та практикою розробки та оптимального використання сучасних або, як їх прийнято називати, нових інформаційних технологій, орієнтованих на реалізацію психолого-педагогічних цілей навчання, виховання.
Процес інформатизації так само торкнувся і економічних галузей. Їх радикальне вдосконалення і пристосування до сучасних умов стало можливим завдяки масовому використанню новітньої комп'ютерної і телекомунікаційної техніки, формування на її основі високоефективних інформаційно-управлінських технологій. Засоби і методи прикладної інформатики використовуються в менеджменті і маркетингу. Нові технології, засновані на комп'ютерній техніці, вимагають радикальних змін організаційних структур менеджменту, його регламенту, кадрового потенціалу, системи документації, фіксування і передачі інформації.
Сучасні інформаційні технології значно розширюють можливості використання інформаційних ресурсів у різних галузях промисловості, а так само в освіті.

Етапи розвитку інформаційних технологій

Загальним для усіх викладених нижче підходів є те, що з появою персонального комп'ютера почався новий етап розвитку сучасних інформаційних технологій. Основною метою стає задоволення персональних інформаційних потреб людини, як для професійної сфери, так і для побутової.

По виду завдань і процесів обробки інформації:

- 1-й етап (60 - 70-і рр..) - Опрацювання даних в обчислювальних центрах у режимі колективного користування. Основним напрямком розвитку інформаційної технології була автоматизація рутинних дій людини.
- 2-й етап (з 80-х рр..) - Створення інформаційних технологій, спрямованих на вирішення стратегічних завдань.

По проблемам, що стоять на шляху інформатизації:

- 1-й етап (до кінця 60-х рр..) - Характеризується проблемою опрацювання великих обсягів даних в умовах обмежених можливостей апаратних засобів.
- 2-й етап (до кінця 70-х рр..) - Пов'язаний з поширенням ЕОМ серії IBM/360. Проблема цього етапу - відставання програмного забезпечення від рівня розвитку апаратних засобів.
- 3-й етап (з початку 80-х рр..) - Комп'ютер стає інструментом непрофесійного користувача, а інформаційні системи - засобом підтримки прийняття його рішень. Проблеми - максимальне задоволення потреб користувача і створення відповідного інтерфейсу для роботи в комп'ютерному середовищі.
- 4-й етап (з початку 90-х рр..) - Створення сучасних інформаційних технологій міжорганізаційних зв'язків та інформаційних систем. Проблеми цього етапу дуже численні. Найбільш істотними з них є:встановлення стандартів, протоколів для комп'ютерного зв'язку; організація доступу до стратегічної інформації; організація захисту і безпеки інформації.

По перевазі, яку надає комп'ютерна технологія:

- 1-й етап (з початку 60-х рр..) - Характеризується досить ефективним опрацюванням інформації при виконанні рутинних операцій з орієнтацією на централізоване колективне використання ресурсів обчислювальних центрів. Основним критерієм оцінки ефективності інформаційних систем була різниця між витраченими на розробку і зекономленими в результаті впровадження коштами. Основна проблема на цьому етапі була психологічна - погана взаємодія користувачів, для яких створювалися інформаційні системи, і розробників через розходження їхніх поглядів і розуміння розв'язуваних проблем. Як наслідок цієї проблеми, створювалися системи, які користувачі погано

сприймали і, незважаючи на їх достатньо великі можливості, не використовували повною мірою.

- 2-й етап (з середини 70-х рр..) - Пов'язаний з появою персональних комп'ютерів. Змінився підхід до створення інформаційних систем - орієнтація зміщається убік індивідуального користувача для підтримки прийнятих ним рішень. Користувач зацікавлений у проведеній розробці, налагоджується контакт із розроблювачем, виникає порозуміння обох груп фахівців. На цьому етапі використовується як централізоване опрацювання даних, характерне для першого етапу, так і децентралізоване, що базується на розв'язанні локальних задач і роботі з локальними базами даних на робочому місці користувача.
- 3-й етап (з початку 90-х рр..) - Пов'язаний з поняттям аналізу стратегічних переваг у бізнесі і заснований на досягненнях телекомунікаційної технології розподіленої обробки інформації. Інформаційні системи мають своєю метою не просто збільшення ефективності опрацювання даних і допомога керівнику. Відповідні інформаційні технології повинні допомогти організації вистояти в конкурентній боротьбі й одержати перевагу.

ВИДИ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Сучасне матеріальне виробництво та інші сфери діяльності все більше потребують інформаційного обслуговування, переробки величезної кількості інформації. Універсальним технічним засобом обробки будь-якої інформації є комп'ютер, який грає роль підсилювача інтелектуальних можливостей людини і суспільства в цілому, а комунікаційні засоби, які використовують комп'ютери, служать для зв'язку і передачі інформації. Поява і розвиток комп'ютерів - це необхідна складова процесу інформатизації суспільства.

Інформатизація суспільства є однією із закономірностей сучасного соціального прогресу. Цей термін все наполегливіше витісняє широко використовуваний до недавнього часу термін «комп'ютеризація суспільства». При зовнішній схожості цих понять вони мають істотну відмінність.

При комп'ютеризації суспільства основна увага приділяється розвитку і впровадженню технічної бази комп'ютерів, що забезпечують оперативне отримання результатів переробки інформації і її накопичення.

При інформатизації суспільства основна увага приділяється комплексу заходів, спрямованих на забезпечення повного використання достовірного, вичерпного і своєчасного знання у всіх видах людської діяльності.

Таким чином, «інформатизація суспільства» є більш широким поняттям, ніж «комп'ютеризація суспільства», і спрямована на якнайшвидше оволодіння інформацією для задоволення своїх потреб. У понятті «інформатизація суспільства» акцент треба робити не стільки на технічних засобах, скільки на

сутності і меті соціально-технічного прогресу. Комп'ютери є базовою технічною складовою процесу інформатизації суспільства.

Інформатизація на базі впровадження комп'ютерних і телекомунікаційних технологій є реакцією суспільства на потребу в істотному збільшенні продуктивності праці в інформаційному секторі суспільного виробництва, де зосереджено більше половини працездатного населення. Так, наприклад, в інформаційній сфері США зайнято понад 60% працездатного населення, в СНД - близько 40%.

З сучасної точки зору використання телефону в перші роки його існування виглядає досить смішно. Керівник диктував повідомлення своєму секретарю, який потім відправляв його з телефонної кімнати. Телефонний дзвінок брали в аналогічній кімнаті іншої компанії, текст фіксували на папері і доставляли адресату. Знадобилося багато часу, перш ніж телефон став таким поширеним і звичним способом повідомлення, щоб його стали, використовувати, так, як ми це робимо сьогодні: самі дзвонимо в потрібне місце, а з появою стільникових телефонів - і конкретній людині.

У наші дні комп'ютери, в основному, застосовуються як засоби створення та аналізу інформації, яку потім переносять на звичні носії (наприклад, папір). Але тепер, завдяки широкому розповсюдженню комп'ютерів і створення Інтернету, вперше можна за допомогою свого комп'ютера спілкуватися з іншими людьми через їх комп'ютери. Необхідність використання роздрукованих даних для передачі колегам усувається подібно до того, як папір зникла з телефонних переговорів. Сьогоднішній день, завдяки використанню Web, можна порівняти з тим часом, коли люди перестали записувати текст телефонних повідомлень: комп'ютери (і їх зв'язок між собою за допомогою Інтернету) вже настільки широко поширені і звичні, що ми починаємо використовувати їх принципово новими способами. WWW - це початок шляху, на якому комп'ютери по - справжньому стануть засобами зв'язку.

Інтернет надає безпрецедентний спосіб отримання інформації. Кожен, хто має доступ до WWW, може отримати всю наявну на ньому інформацію, а також потужні засоби її пошуку. Можливості для освіти, бізнесу та зростання взаєморозуміння між людьми стають просто приголомшливими. Більше того, технологія Web дозволяє поширювати інформацію всюди. Простота цього способу не має аналогів в історії. Для того щоб зробити свої погляди, товари або послуги відомими іншим, більше немає необхідності купувати простір в газеті чи журналі, платити за час на телебаченні і радіо. Web робить правила гри однаковими для уряду і окремих осіб, для малих і великих фірм, для виробників і споживачів, для благодійних і політичних організацій. World Wide Web (WWW) в інтернеті - це найдемократичніший носій інформації: з його допомогою будь-хто може сказати і почути сказане без проміжної інтерпретації, спотворення і цензури, керуючись певними рамками пристойності. Інтернет забезпечує унікальну свободу самовираження особистості та інформації.

Подібно до використання внутрішніх телефонів компаній для зв'язку співробітників між собою і зовнішнім світом, Web застосовується як для зв'язку всередині організації, так і між організаціями та їх споживачами, клієнтами і партнерами. Та ж сама технологія Web, яка дає можливість невеликим фірмам заявити про себе на Інтернеті, великою компанією може використовуватися для передачі даних про поточний стан проекту по внутрішній інтрамережі, що дозволить її співробітникам завжди бути більш обізнаними і, отже, більш оперативними в порівнянні з невеликими , моторними конкурентами. Застосування інтрамережі всередині організації для того, щоб зробити інформацію доступнішою для своїх членів, також є кроком вперед у порівнянні з минулим. Тепер, замість того, щоб зберігати документи в заплутаному комп'ютерному архіві, з'явилася можливість (під контролем засобів захисту) легко проводити пошук і опис документів, робити посилання на них і складати покажчики. Завдяки технології Web бізнес, так само як і управління, стає більш ефективним.

ПРОБЛЕМИ І ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Старіння інформаційної технології

Для інформаційних технологій є цілком природним те, що вони застарівають і заміняються новими.

Так, наприклад, на зміну технології пакетної обробки програм на великий ЕОМ в обчислювальному центрі прийшла технологія роботи на персональному комп'ютері на робочому місці користувача. Телеграф передав всі свої функції телефону. Телефон поступово витісняється службою експрес доставки. Телекс передав більшість своїх функцій факсу й електронній пошті.

При впровадженні нової інформаційної технології в організації необхідно оцінити ризик відставання від конкурентів у результаті її неминучого старіння з часом, тому що інформаційні продукти, як ніякі інші види матеріальних товарів, мають надзвичайно високу швидкість змінюваності новими видами або версіями. Періоди змінюваності коливаються від декількох місяців до одного року. Якщо в процесі впровадження нової інформаційної технології цьому фактору не приділяти належної уваги, можливо, що до моменту завершення перекладу фірми на нову інформаційну технологію вона вже застаріє і прийдеться вживати заходів до її модернізації. Такі невдачі з впровадженням інформаційних технологій звичайно пов'язують з недосконалістю технічних засобів, тоді як основною причиною невдач є відсутність або слабка пропрацьованість методології використання інформаційної технології.

Методологія використання інформаційної технології

Централізована обробка інформації на ЕОМ обчислювальних центрів була першою історично сформованою технологією. Створювалися великі обчислювальні центри колективного користування, оснащені великими ЕОМ (у

нашій країні - ЕОМ ЄС). Застосування таких ЕОМ дозволяло обробляти великі масиви вхідної інформації й одержати на цій основі різні види інформаційної продукції, яка потім передавалася користувачам. Такий технологічний процес був обумовлений недостатнім оснащенням обчислювальною технікою підприємств і організацій в 60 - 70-і рр..
Переваги методології централізованої технології:

- Можливість звернення користувача до великих масивів інформації у вигляді баз даних і до інформаційної продукції широкої номенклатури;
- Порівняльна легкість впровадження методологічних рішень по розвитку й удосконаленню інформаційної технології завдяки централізованому прийняттю

Недоліки такої методології:

- Обмежена відповідальність нижчого персоналу, який не сприяє оперативному одержанню інформації користувачем, тим самим, перешкоджаючи правильності виробітку управлінських рішень;
- Обмеження можливостей користувача в процесі одержання і використання інформації.

Децентралізована обробка інформації пов'язана з появою в 8О-х рр.. персональних комп'ютерів і розвитком засобів телекомунікацій. Вона дуже істотно потіснила попередню технологію, оскільки дає користувачу широкі можливості в роботі з інформацією і не обмежує його ініціатив.
Перевагами такої методології є:

- Гнучкість структури, що забезпечує простір ініціативам користувача;
- Посилення відповідальності нижчої ланки співробітників;
- Зменшення потреби в користуванні центральним комп'ютером і відповідно контролі з боку обчислювального центру;
- Більш повна реалізація творчого потенціалу користувача завдяки використанню засобів комп'ютерного зв'язку.

Проте ця методологія має і свої недоліки:

- Складність стандартизації через велику кількість унікальних розробок;
- Психологічне неприйняття користувачами рекомендованих обчислювальним центром стандартів готових програмних продуктів;
- Нерівномірність розвитку рівня інформаційної технології на локальних місцях, що в першу чергу визначається рівнем кваліфікації конкретного працівника.

Описані переваги і недоліки централізованої і децентралізованої інформаційної технології призвели до необхідності дотримуватися лінії розумного застосування і того, і іншого підходу.
Такий підхід назвемо раціональною методологією і покажемо, як у цьому випадку будуть розподілятися обов'язки:

- Обчислювальний центр повинен відповідати за вироблення загальної стратегії використання інформаційної технології, допомагати користувачам, як у роботі, так і в навчанні встановлювати стандарт і визначати політику застосування програмних і технічних засобів;
- Персонал, який використовує інформаційну технологію, повинен дотримуватися вказівок обчислювального центру, здійснювати розробку своїх локальних систем і технологій відповідно до загального плану організації.

Раціональна методологія використання інформаційної технології дозволить досягти більшої гнучкості, підтримувати загальні стандарти, здійснити сумісність інформаційних локальних продуктів, знизити дублювання діяльності та ін

Перспективи розвитку інформаційних технологій в Україні

Інформаційна технологія – це сукупність методів, виробничих процесів та програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує виконання інформаційних процесів з метою підвищення їхньої надійності та оперативності і зниження трудомісткості ходу використання інформаційного ресурсу.

Інформаційні технології – одні з найважливіших досягнень діяльності людства. Використання інформаційних технологій дає можливість створити сприятливі умови для розвитку економіки, стимулювати зростання продуктивності праці та підвищення заробітної платні, полегшити організацію комунікацій на всіх рівнях управління, швидко знижувати матеріало- та енергоємність окремого виробництва і національної економіки в цілому.

Розвиток сфери новітніх технологій зробив великий внесок у створення інформаційних систем. Для України дуже важливо, що застосування інформаційних технологій дає можливість підвищити якість підготовки і прийняття важливих рішень виконавчої влади. З 2000 р. Україна активно включилася в становлення інформаційного суспільства. У 2007 р. був прийнятий закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки».

Основним завданням розвитку інформаційного суспільства в Україні є сприяння кожній людині на засадах широкого використання сучасних ІКТ можливостей створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізовуючи свій потенціал, підвищуючи якість свого життя. Розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визначається одним з пріоритетних напрямів державної політики.

Національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах: пріоритетності науково-технічного та інноваційного

розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов; всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та ІКТ; сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу; посилення мотивації щодо використання ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечення інформаційної безпеки.

Але на шляху досягнення цих цілей виникають труднощі пов’язані з недостатньою технологічною базою, складним фінансовим забезпеченням цього процесу, відсутністю достатньої кількості наукових досліджень процесу формування інформаційного суспільства і його складових.

Сучасна інформаційна система дозволяє забезпечити:

1) прямий і своєчасний доступ до інформаційного продукту;
2) ефективну координацію внутрішньої діяльності;
3) використання якісно кращої технології системного аналізу та проектування оперативного управління на різних ланках діяльності підприємства тощо.

Україна накопичила значний потенціал в інформаційних технологіях. Її національною конкурентною перевагою є діяльність з їх розробки. Але Україна як товаровиробник може бути витиснута з найбільш перспективних світових ринків через відсутність обґрунтованої державної політики. Розробка інформаційного суспільства в Україні має базуватися на узгодженості дій усіх гілок влади. Розв’язання проблем відсталості інформаційних технологій в Україні вимагає загальнодержавного підходу, а саме:

1) формування національної стратегії, міжнародної і внутрішньої політики, сприятливої законодавчої, суспільної, економічної атмосфери у сфері використання інформаційних технологій;
2) забезпечення потенціальної можливості технологічного доступу населення до інформаційних комп’ютерних технологій за рахунок об’єднання зусиль державного та приватного секторів економіки щодо розвитку інформаційної інфраструктури;
3) сприяння збільшенню і розповсюдженню кількості послуг населенню і бізнесу, наданих за допомогою інформаційних комп’ютерних технологій;
4) концентрація зусиль держави і суспільства для створення загальнодоступних електронних ресурсів на основі врахувань національних, політичних, економічних. Мовних, культурних та релігійних аспектів розвитку України;
5) забезпечення можливості отримання знань, умінь і навичок використання інформаційних комп’ютерних технологій у процесі одержання освіти.

Нашій країні необхідна певна політика у сфері інформатизації, бо в Україні є ще деякі перешкоди які варто усунути, а саме:

1) гостра нестача кваліфікованих кадрів;
2) непридатність існуючої моделі відношення до інформаційних технологій з боку влади для впевненого збереження досягнутих позицій на світовому ринку;
3) недієвість захисту прав інтелектуальної власності;
4) занадто дорога й неякісна інфраструктура.

Інформаційне суспільство - комплексне поняття, що складається з множини різноманітних аспектів. Щоб залишатися конкурентоспроможними в умовах прогресивного еволюційного ринку, необхідно використовувати всі переваги новітніх технологій.

Список використаної літератури:

1. Єдинак В.С. Розвиток інформаційних технологій в Україні.//Наукові доробки молоді – вирішенню проблем європейської інтеграції: збірник наукових статей.В 2 т. Т. 1- Харків: Континент, 2008.- С. 289-290.
2. Пацай Б.Д. Роль інформаційних технологій в управлінні фінансовими ресурсами підприємств.// Фінанси України. - № 8 – 2008. – С.82-84.
3. Шандра В.М. Застосування інформаційних технологій в забезпеченні технологічного оновлення економіки на інноваційній основі.// Актуальні проблеми економіки. - №10 – 2007. – С.220-223.
4. Чигасова Н.М. Місце інформаційних технологій у розвитку інформаційного суспільства в Україні.// Формування ринкових відносин в Україні: Збірник наукових праць. - № 9 – 2007. – С. 110-113.

Баргилевич Олександр Анатолійович
Шитіков Микита Андрійович
Державний університет Телекомунікацій
Факультет телекомунікацій
м. Київ

ЗНАЧИМІСТЬ ІНФОРМАТИКИ В СУЧАСНОМУ ЖИТТІ

1) Інформатика це — наукова дисципліна, що вивчає методи та процеси створення, перетворення, зберігання, передачі інформації та використання її в різних галузях людської діяльності. На сьогоднішній день інформатика як наука розвивається швидше ніж інші галузі.

У даній статті ми розглядаємо потрібність на важливість предмета інформатики та інформатики в цілому у житті людини. Описуємо де можна використовувати

набуті знання і навички з цього предмета. Також пояснюється важливість вивчення алгоритмів та їх використання в повсякденному житті.

2) В результаті проведеного дослідження виявили по-перше, інформатика — у міжгалузевому науковому розумінні розглядається як багатозначна, багатофункціональна категорія. По-друге, за сутністю інформатика має триєдиний зміст: 1- як міжгалузева наука; 2- як навчальна дисципліна; 3- як сфера суспільних відносин, що знайшла відображенні у інформаційному праві. По-третє Основне теоретичне завдання інформатики полягає у визначенні загальних закономірностей, відповідно до яких створюється інформація, відбувається її перетворення, передавання та використання у різних сферах діяльності людини. Також прикладні завдання інформатики полягають у розробці найефективніших методів і засобів здійснення інформаційних процесів, у визначенні способів оптимальної наукової комунікації у самій науці та між наукою і виробництвом.

3) Висновком проведеного дослідження є виявлення значимості інформатики, інформації та інформаційних технологій у сферах людської діяльності. Сучасне суспільство наповнене і пронизане потоками інформації, які потребують обробки.

Історія

Незважаючи на свій юний вік (а сучасна інформатика, набула свого бурхливого розвитку порівняно недавно — у другій половині XX ст.), її дескриптологічні корені простягаються далеко в минуле, коли вперше виникла ідея формалізації розумової діяльності людини. Перший крок у цьому напрямі зробив Арістотель (384—322 рр. до н. е.) у теорії силогізмів. Значно пізніше, тільки через півтори тисячі років, було зроблено наступний крок і висунуто загальну ідею механізації логічних умовиводів і відокремлення їх від мозку людини. Вона належала іспанському (каталонському) логіку Раймунду Луллію (1235—1315), який поставив задачу на основі Аристотелевої логіки розробити універсальний метод пізнання й механізувати його за допомогою спеціальної машини, яка б моделювала силогічні виведення. Хоча Р. Луллію не вдалося до кінця реалізувати свій задум і побудувати таку машину, сама ідея і спроба моделювання та механізації логічних умовиводів стала піонерською в галузі створення штучних обробників інформації.

Принциповим кроком на шляху до інформатики було створення спеціальних інтенсіональних дескриптивних систем, призначених для уточнення й вивчення загальних властивостей інтуїтивного до цього поняття алгоритму та обчислюваної функції. Серед перших таких систем були лямбда-числення А. Чорча(1936), машини Тьюрінга (1936), алгоритми Поста (1936) тощо. Згодом було доведено, що в певному сенсі всі ці моделі алгоритмів еквівалентні. Уточнення поняття алгоритму дозволило виділити клас алгоритмічно розв'язних задач. Для багатьох

задач була доведена їхня алгоритмічна нерозв'язність. Перший приклад такої задачі навів А. Чорч (1903—1995), який довів нерозв'язність чистого прикладного числення предикатів.

В 1945 з'явилась стаття американського вченого та інженера В. Буша «Можливий механізм нашого мислення», в якій вперше широко ставилось питання про необхідність механізації інформаційного пошуку. Міжнародні конференції з наукової інформації (Лондон, 1948; Вашингтон, 1958) знаменували перші етапи розвитку інформатики. До середини 60-х років 20 століття розроблялись в основному принципи і методи інформаційного пошуку та технічні засоби їхньої реалізації. У. Баттен, К. Муерс і М. Таубе заклали основи координатного індексування; Б. Вікері, Д. Фоскет, Дж. Перрі, А. Кент, Дж. Костелло, Г. П. Лун, Ч. Берньер, Ж. К. Гарден розробили основи теорії і методики інформаційного пошуку. С. Клевердон вивчив методи порівняння технічної ефективності інформаційно-пошукових систем різного типу. Р. Шоу і Ж. Самен створили перші інформаційно пошукові пристрої на мікрофільмах і діамікрокартах, що стали прообразами багатьох спеціальних інформаційних машин. К. Мюллер і Ч. Карлсон запропонували нові методи репродукування документів, які лягли в основу сучасної техніки репрографії.

Сучасний етап розвитку характеризується глибшим розумінням загальнонаукового значення науково-інформаційної діяльності та все ширшим застосуванням у ній електронних обчислювальних машин.

Інформа́тика — наукова дисципліна, що вивчає методи та процеси створення, перетворення, зберігання, передачі інформації та використання її в різних галузях людської діяльності.

Основне теоретичне завдання інформатики полягає у визначенні загальних закономірностей, відповідно до яких створюється інформація, відбувається її перетворення, передавання та використання у різних сферах діяльності людини.

Як дисципліна, інформатика охоплює широке коло тем від теоретичних досліджень алгоритмів і меж обчислень до практичної реалізації обчислювальних систем в області апаратного та програмного забезпечення.

Важливість предмета інформатики на першому курсі ВИШу. Важливість в цілому

Хорошим ІТ спеціалістом може стати кожен. Дуже важливим є предмет інформатики на першому курсі. Саму у період навчання людина отримує базові знання, без яких не може бути хорошого програміста - вивчення сучасних

технологій автоматизації проектування систем, продуктів і сервісів IT, сучасних парадигм і різноманітних мов програмування, вивчення безлічі стандартів, методів і засобів управління безпекою IT і управління розподіленими ресурсами.

Сьогодні в світі немає жодної галузі науки і техніки, яка розвивалася б так само стрімко, як інформатика. Роль інформатики в розвитку суспільства надзвичайно велика. З нею пов'язаний початок революції в області накопичення, передачі та обробки інформації. Ця революція, наступна за революціями в оволодінні речовиною і енергією, зачіпає і докорінно перетворює не тільки сферу матеріального виробництва, а й інтелектуальну, духовну сфери життя.

Роль інформатики в сучасних умовах постійно зростає. Діяльність як окремих людей, так і цілих організацій все більшою мірою залежить від їх інформованості і здатності ефективно використовувати наявну інформацію. Впровадження комп'ютерів, сучасних засобів переробки і передачі інформації в різні індустрії послужило початком процесу, званого інформатизацією суспільства. Сучасне матеріальне виробництво та інші сфери діяльності все більше потребують інформаційному обслуговуванні, переробці величезної кількості інформації.

Результатом процесу інформатизації є створення інформаційного суспільства, де маніпулюють матеріальними об'єктами, ідеями, образами, інтелектом, знаннями. Для кожної країни її рух від індустріального етапу розвитку до інформаційного етапу визначається ступенем інформатизації суспільства.

Де можливе використання знань і навичок

Зовсім недавно кар'єра IT фахівця була приблизно так: технічна підтримка користувачів, системне адміністрування, розробка програмного забезпечення, керівник проектної групи, начальник відділу автоматизації або менеджер вищої ланки в області IT-технологій.

Сьогодні способів для самореалізації в сфері IT набагато більше. Наприклад, розробники можуть займатися бізнес-аналізом і консалтингом, потім перейти в проектне управління або IT-менеджмент. Сьогодні високо цінуються фахівці - прикладники з якісною IT-освітою та економічними знаннями.

Фахівці в сфері IT були завжди затребувані і попит на них тільки збільшується з кожним роком, що говорить про хорошу перспективу для цих професій. Найбільшого успіху в пошуку роботи домагаються комунікабельні фахівці з хорошим знанням англійської мови та досвідом роботи близько року. Навчання в зарубіжних вузах збільшує шанси.

Інформатика - комплексна наукова дисципліна з широким діапазоном застосування. Її пріоритетними напрямками є

1)розробка обчислювальних систем і програмного забезпечення;

2) теорія інформації, що вивчає процеси, пов'язані з передачею, прийомом, перетворенням і зберіганням інформації;

3) математичне моделювання, методи обчислювальної і прикладної математики та їх застосування до фундаментальних і прикладних досліджень в різних областях знань;

4) методи штучного інтелекту, що моделюють методи логічного та аналітичного мислення в інтелектуальній діяльності людини (логічний висновок, навчання, розуміння мови, візуальне сприйняття, ігри та ін.);

5) системний аналіз, який вивчає методологічні засоби, що використовуються для підготовки та обгрунтування рішень щодо складних проблем різного характеру;

6) біоінформатика, яка вивчає інформаційні процеси в біологічних системах;

7) соціальна інформатика, що вивчає процеси інформатизації суспільства;

8) методи машинної графіки, анімації, засоби мультимедія;

9) телекомунікаційні системи і мережі;

10) різноманітні програми, що охоплюють виробництво, науку, освіту, медицину, торгівлю, сільське господарство і всі інші види господарської та громадської діяльності.

Важливість вивчення алгоритмів

Скільки існує різних завдань, стільки існує і різних алгоритмів для їх вирішення. Проте є велика ймовірність того що завдання яке ви намагаєтеся вирішити в деякому сенсі схоже на іншу задачу. Розвиваючи глибоке розуміння широкого діапазону алгоритмів, ви зможете вибрати вірний алгоритм і застосувати його для вирішення завдання.

Перший крок до розуміння важливості вивчення і знання алгоритмів це дати точне визначення того, що розуміється під алгоритмом. Згідно популярній книзі «Алгоритми: побудова й аналіз (Кормен, Лейзерсон, Ривест, Штайн)» «алгоритм (algorithm) - це будь-яка коректно певна обчислювальна процедура, на вхід (input) якої подається деяка величина або набір величин, і результатом виконання якої є вихідна (output) величина або набір значень ». Іншими словами, алгоритми схожі на дорожні карти для досягнення чітко визначеної задачі. Частина коду, для

обчислення членів послідовності Фібоначчі - це реалізація конкретного алгоритму. Навіть проста функція складання двох чисел є алгоритмом, хоча і простим.

Чому важливо знати алгоритми

Щоб використовувати алгоритми належним чином, важливо знати всі типи алгоритмів. Якщо вам доведеться розробляти важливу частину програмного забезпечення, то ви повинні бути в змозі оцінити швидкість роботи вашого алгоритму. Точність вашої оцінки залежить від того наскільки ви володієте аналізом часу виконання алгоритмів. Крім цього, необхідно знати деталі алгоритмів, що дозволить передбачати особливі випадки, в яких програма не працюватиме швидко, або буде давати неприйнятні результати.

Звичайно, будуть моменти, коли ви будете мати справу з проблемами з якими раніше не стикалися. У таких випадках потрібно придумати новий алгоритм, або по-новому застосувати старий алгоритм. Чим більше ви знаєте про алгоритми, тим більше у вас шансів знайти хороше рішення проблеми. У багатьох випадках нова задача легко зводиться до старої, але для цього потрібно мати фундаментальне розуміння старих завдань.

Приклад

Як приклад можна розглянути, як працюють мережеві комутатори. Комутатор має N підключених до нього кабелів, і приймає пакет даних, що надходять з цих кабелів. Комутатор повинен спочатку проаналізувати пакети, а потім відправити їх назад по правильному кабелю. Комутатор також як і комп'ютер працює в дискретному режимі - пакети відправляються дискретними інтервалами, а не безперервно. Швидкий комутатор прагне послати, як можна більше пакетів протягом кожного інтервалу інакше вони накопичаться і комутатор «впаде». Мета алгоритму відправляти максимальну кількість пакетів протягом кожного інтервалу, а також забезпечити порядок, при якому пакети, що прийшли раніше за інших відправлялися теж раніше інших. Такі зв'язки між завданням і рішенням можна виявити тільки за допомогою вже наявних алгоритмічних знань.

Приклади рішень реальних завдань вимагають новітніх алгоритмів предостатньо. Майже все, що ви робите на комп'ютері залежить від алгоритмів, які хтось дуже довго розробляв. Навіть найпростіших програм не існувало б без алгоритмів, які

працюють «за сценою» керуючи пам'яттю і завантажуючи дані з жорсткого диска.

Інформаційне суспільство

В даний момент інформатика вже сильно влилася у суспільство і створила інформаційне суспільство – соціологічна концепція, що визначає головним фактором розвитку суспільства виробництво та використання науково-технічної та іншої інформації. Концепція інформаційного суспільства є різновидом теорії постіндустріального суспільства, засновниками якої були З.Бжезинський, О.Белл, О.Тоффлер.

Концепція і термінологія «інформаційного суспільства» набули значного поширення в Україні услід за їх поширенням у світі з тими ж, характерними для світу, протиріччями та неясностями у їх застосуванні. Термін «інформаційне суспільство» у більшості випадків використовується як яскравий синонім терміну «інформаційно-комунікаційні технології», а концепція «інформаційного суспільства», і до сьогодні, не отримала глибокого осмислення і адаптації під українські реалії внаслідок занепаду української науки.

Вперше орієнтацію України на створення «інформаційного суспільства» було офіційно зафіксовано в Стратегії інтеграції України до ЄС (розділ 13), ухваленою в 1998 році. Варто відзначити, що одночасно, в 1998 році було прийнято два Закони України «Про Концепцію Національної програми інформатизації» та «Про Національну програму інформатизації», якими визначалися принципи і програма дій інформатизації України, а не побудови в ній «інформаційного суспільства». Таке протиріччя у концептуальних основах між різними групами фахівців і політиків на найвищому рівні прийняття політичних рішень в Україні свідчить про некритичність сприйняття іноземних новацій. Воно сильно зашкодило практиці інформаційно-комунікаційного розвитку України.

Крім того, населення лишається незахищеним від інформаційних впливів, а суспільство в цілому - від інформаційних загроз. Так, відповідно до положень ст. 7 Закону України Про основи національної безпеки України від 19.06.2003 № 964-IV, в інформаційній сфері існують такі загрози національній безпеці держави: - прояви обмеження свободи слова та доступу громадян до інформації; - поширення засобами масової інформації культу насильства, жорстокості, порнографії; - комп'ютерна злочинність та комп'ютерний тероризм; - розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; - намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Україні іще належить виконати значний обсяг роботи з осмислення і адаптації концепції «інформаційного суспільства» в українських реаліях, розроблення та

реалізації Національної стратегії сучасного інформаційно-комунікаційного розвитку (а не «інформаційного суспільства»). Прикладом для такої роботи є досвід Фінляндії, висвітлений у книзі за співавторством одного із класиків «інформаційного суспільства» — Мануеля Кастельса, дбайливо перекладеній на українську мову.

Висновок. Сучасне суспільство навряд чи можна уявити без інформатики. Перспективи розвитку обчислювальної техніки сьогодні складно уявити навіть фахівцям. Проте, ясно, що в майбутньому нас чекає щось грандіозне. І якщо темпи розвитку інформатики і інформаційних технологій не скоротяться (а в цьому немає ніяких сумнівів), то це відбудеться дуже скоро.Сучасне суспільство наповнене і пронизане потоками інформації, які потребують обробки. Тому без інформаційних технологій та інформатики так само як без енергетичних, транспортних і хімічних технологій, воно нормально функціонувати не може.

Джерела:

1. Вікіпедія

2. Бочкін А.І. Методика викладання інформатики: Учеб. посібник. - Мінськ: Вишейш. шк., 1998.

3. Алгоритми: побудова й аналіз (Кормен, Лейзерсон, Ривест, Штайн)

Пикуль Анна Руслановна
Государственный Университет Телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ОБЛАЧНЫЕ ХРАНИЛИЩА ДАННЫХ

Облачное хранилище данных (cloud storage) — модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут располагаться удалённо друг от друга географически.
Преимущества:

- Возможность доступа к данным с любого компьютера, имеющего выход в интерент;

- Возможность организации совместной работы с данными
- Высокая вероятность сохранения данных даже в случае аппаратных сбоев
- Клиент платит только за то место в хранилище, которое фактически использует, но не за аренду сервера, все ресурсы которого он может и не использовать.
- Клиенту нет необходимости заниматься приобретением, поддержкой и обслуживанием собственной инфраструктуры по хранению данных, что, в конечном счёте, уменьшает общие издержки производства.
- Все процедуры по резервированию и сохранению целостности данных производятся провайдером «облачного» центра, который не вовлекает в этот процесс клиента.

Недостатки:

- Безопасность при хранении и пересылке данных является одним из основных вопросов при работе с «облаком», особенно в отношении конфиденциальных и приватных данных. Так например провайдер имеет возможность просматривать данные клиента (если они не защищены паролем), которые также могут попасть в руки хакеров, сумевших взломать системы защиты провайдера.
- Надёжность, своевременность получения и доступность данных в «облаке» очень сильно зависит от многих промежуточных параметров, таких как: каналы передачи данных на пути от клиента к «облаку», надежность последней мили, качество работы интернет-провайдера клиента, доступность самого «облака» в данный момент времени. Если же сама компания предоставляющая онлайновое хранилище будет ликвидирована, клиент может потерять все свои данные.
- Общая производительность при работе с данными в «облаке» может быть ниже, чем при работе с локальными копиями данных.
- Абонентская плата за дополнительные возможности (увеличенный объем хранения данных, передача больших файлов и т. д.)

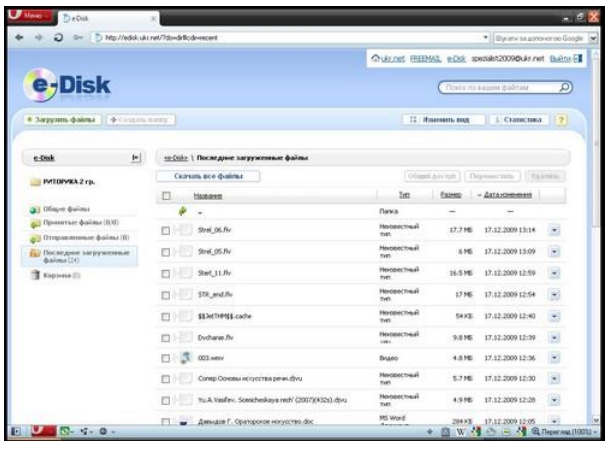
Аналитики во весь голос твердят, что будущее IT-рынка – это облачные технологии. За последние 4 года на рынке появились десятки пользовательских облачных сервисов, которые предлагают всевозможные плюшки, будь то увеличенное дисковое пространство, наличие шифрования данных или клиента для мобильных

устройств.

Dropbox

Сервис, с аудиторией в 100 млн пользователей. Это самый популярный сервис, с которым знакомы практически все пользователи, которые когда-либо интересовались темой «облаков». При регистрации на сервисе, Dropbox интегрируется в операционную систему, создавая папку с одноименным названием. Таким образом, поместив в папку любой файл, он будет загружен на сервер облака. Фактически, пользователю даже не нужен веб-интерфейс. Для тех, кто использует мобильные устройства, Dropbox разработал клиенты для iPhone, iPad, Android, BlackBerry и Kindle Fire. Правда, не предусмотрена поддержка Symbian и Windows Mobile. По неофициальной информации, Microsoft не пустила Dropbox из-за продвижения собственного хранилища SkyDrive.
Бесплатно предоставляется 2 ГБ онлайн-хранилища. По количеству дискового пространства Dropbox проигрывает многим сервисам, но за счет реферальной программы приглашения пользователей можно довести объем виртуального пространства на облаке до 18 Гб (по 500 Мб за друга). Стоимость аккаунта Pro на 100 ГБ обойдется в $9,99 ежемесячно, 200 ГБ – $19,99 и 500 ГБ – $49,99. Важным моментом является создание публичных ссылок, которые будут доступны всем пользователям, независимо от того, являются ли они клиентами сервиса Dropbox или нет. В тоже время, многие пользователи жалуются на скорость загрузки файлов на сервер, а также долгое время ожидания окончания синхронизации, которое может составлять десятки минут.

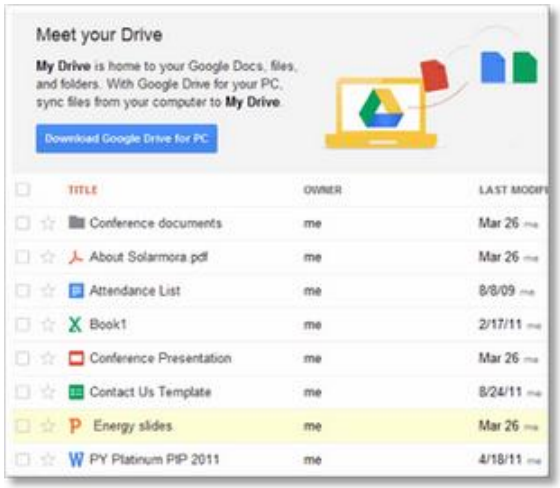
e-Disk



Виртуальная флешка от портала Ukr.net и украинская альтернатива нашумевшим иностранным облачным аналогам. e-Disk – это персональное хранилище файлов объемом в 4 ГБ. После того, как пользователь зарегистрировался на сайте сервиса, перед ним появляется подсказка, как пользоваться сервисом, в картинках. Эта функция будет полезна

для тех, кто только начинает осваивать облачные технологии. Плата за использование сервиса не требуется. Плюсом e-Disk является возможность загрузки файлов любых расширений до 1,5 ГБ, а также неограниченное время хранения файлов на сервере. Правда для этого, пользователю необходимо как минимум раз в 3 месяца посещать облачный сервис. Существует возможность входа в сервис с помощью мобильного браузера, однако нет мобильных клиентов, что можно занести в пассив e-Disk. Тем не менее, облачное хранилище данных от портала Ukr.net позволяет предоставлять загруженные файлы или папки друзьям. Главное, чтобы они были зарегистрированы на Ukr.net.

Google Drive

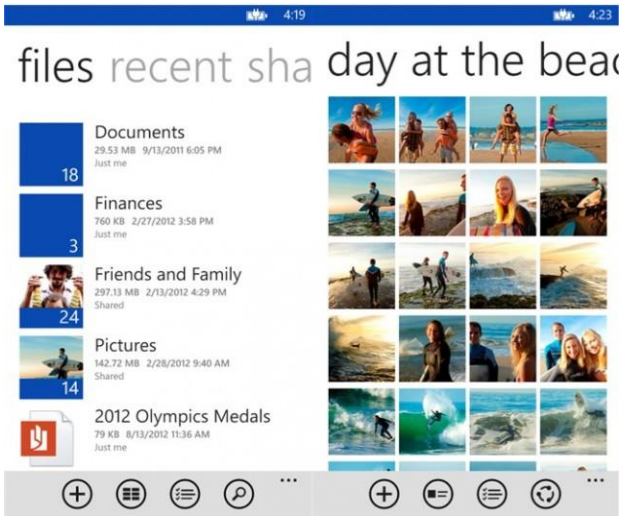


Облачное хранилище, которое долгое время пребывало в ранге перспективного из-за того, что его создателем является поисковый гигант, компания Google. Стартовый объем Google Drive, который предоставляется бесплатно, составляет 5 ГБ. Платные тарифные планы начинаются с $2,49 за месяц за 25 ГБ или $4,99 за 100 ГБ. Из особенностей функционала стоит отметить интеграцию с сервисом Google Docs, а также почтой Gmail и социальной сетью Google+. Также в Google Drive предусмотрена функция резервного копирования – по умолчанию сохраняются все изменения внесенные за последние 30 дней. Интерфейс веб-управлением облачным хранилищем достаточно удобен и функционален. Среди минусов стоит отметить лицензионное соглашение на передачу всего пользовательского контента компании Google и ее партнерам.

iCloud

Сервис iCloud нельзя назвать облачным хранилищем, в классическом понимании этого словосочетания.

Это ретинкарнация провалившегося проекта Me.com, в которую разработчики вдохнули новую жизнь. Этот облачный сервис рассчитан исключительно для внутреннего пользования почитателей продукции Apple, будь то iPad, iPhone, iPod touch или Mac. Сервис сохраняет пользовательский контент и предоставляет доступ к фотографиям, календарям, контактам и документам, а также другим материалам на любом устройстве. Веб-версия сервиса включает в себя пять разделов: «почта», «календарь», «контакты», «найти iPhone» и iWork, в то время как мобильная версия приложения включает в себя на порядок больше разделов. Каждый новый пользователь получает при регистрации 5 ГБ дискового пространства. В качестве компенсации пользователям MobileMe, компания Apple дарит 20 ГБ на один год. Что касается платных пакетов, то жители Европейского Союза могут получить дополнительно 10 ГБ за 16 евро в год, 20 ГБ за 32 евро и 50 ГБ за 80 евро в год.



Microsoft SkyDrive

Выход облачного сервиса от известной компании-разработчика пользователи ждали с нетерпением. Но, как правило, ожидания не всегда оправдываются. Сервис был создан в 2007 году и с тех пор пережил ряд кардинальных изменений и обновлений. Каждому пользователю при регистрации предоставляется 7 ГБ дискового пространства, а пользователям, владеющим лицензиями на продукты Microsoft, можно рассчитывать на 25 ГБ облачного хранилища. Файлы в SkyDrive сохраняются в достаточно структурированном виде. По умолчанию доступны 3 папки: «Документы», «Общая» и «Фотографии». Изначально, сервис был доступен на Windows Phone 7, потом было выпущено приложение для iOS, позже для Windows и наконец для Mac. Если пользователь хочет загрузить файл в хранилище, то ограничение на загрузку одного файла составит 300 МБ. Мобильный клиент позволяет загрузить только фотографии и видеозаписи,

оставляя за бортом документы. Также, в SkyDrive трудно с поддержкой linux, вернее ее просто нет.

Яндекс.Диск

Облачный сервис от компании «Яндекс» сравнительно недавно влился в этот рынок, но уже может похвастаться прочными позициями среди русскоговорящей аудитории Интернета. В частности, популярность пользователей была завоевана благодаря щедрой раздаче дискового пространства. С бесплатной учетной записью, пользователь в общей сложности может получить 10 ГБ. Но для этого нужно постараться. Изначально пользователю доступно 3 ГБ. Далее при регистрации на сервисе, который является не отдельным облачным хранилищем, а частью «Яндекс.Почта», пользователю необходимо пройти небольшой квест, за который он будет награжден 10 ГБ виртуального пространства. Сначала нужно загрузить программу «Диска» на компьютер, далее отправить на сервер несколько файлов и отправить ссылку на сервис по почте, или разместить в социальных сетях. Программы для работы с «Диском» доступны для Windows, Mac OS, Android и iOS. Русскоязычные пользователи сети Интернет часто хвалят виртуальную флешку от компании «Яндекс» за ее быстроту, что немаловажно в передаче данных. Стоит отметить, что отдельного клиента для «Яндекс.Диска» не предусмотрено – на мобильных устройствах возможность доступа к сервису завязана на клиент «Яндекс.Почты».

Сравнительная таблица облачных хранилищ данных

Сервис	Бесплатный объем (ГБ)	ОС	Тарифы
Dropbox	2 (до 18 с помощью реферальной программы)	Веб-интерфейс, Microsoft Windows, OS X, Android, iOS, BlackBerry	$9,99 – 100 ГБ (в месяц);$19,99- 200 ГБ;$49,99 – 500 ГБ;
e-Disk	4	Веб-интерфейс	Бесплатно
Google Drive	5	Веб-интерфейс, Microsoft Windows, OS X, Android, iOS	$2,49 – 25 ГБ (в месяц); $4,99 – 100 ГБ;
iCloud	5 (20 ГБ дарит Apple в качестве компенсации пользователям MobileMe)	Веб-интерфейс, iOS	16 евро – 10 ГБ (в год);32 евро – 20 ГБ; 80 евро – 50 ГБ;
Microsoft SkyDrive	7 (25 – для пользователей, владеющих лицензиями на продукты Microsoft)	Веб-интерфейс, Microsoft Windows, Ubuntu, Android, iOS	$11 – 20 ГБ (в год);$27 – 50 ГБ;$54 – 100 ГБ;
«Яндекс.Диск»	3 (бесплатное расширение до 10)	Веб-интерфейс, Microsoft Windows, OS X, Linux, Android, iOS	Бесплатно

Соснова Дана Назарівна
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

BYOD – ЧЕТЫРЕ БУКВЫ СПОСОБНЫЕ НАПУГАТЬ ДАЖЕ КРУПНУЮ КОМПАНИЮ

В этом году на многих технологичных сайтах все чаще мелькает аббревиатура BYOD (BringYourOwnDevice) – "Возьми Свое Собственное Устройство на работу"

Почему свой мобильник ближе к телу или почему сотрудники все чаще приносят на работу свои собственные устройства? BYOD – модный западный тренд, который очень быстро завоевывает отечественные просторы.Сегодня мы можем наблюдать, процесс естественного отбора в действии: новые компактные и мощные устройства вытесняют морально устаревшие настольные ПК, как в свое время более совершенные виды вытеснили динозавров, долгое

время господствующих на Земле. Мобильные девайсы стали частью повседневности и без них мы уже не представляем нашу жизнь. Многие из нас проделывая путь на работу, или находясь дома, используют свои смартфоны и планшеты для общения с друзьями и решения различных задач.

Как показывает практика, все большее количество сотрудников компаний пользуются на рабочем месте своими собственными мобильными устройствами. В этом году на многих технологичных сайтах все чаще мелькает аббревиатура BYOD (BringYourOwnDevice) – "Возьми Свое Собственное Устройство на работу". Это модный тренд, который очень быстро завоевывает отечественные просторы. В западных компаниях, где когда-то было царство корпоративных BlackBerry, рост мобильного зоопарка стал просто шоком для IT-служб. В Украине это, пока, не стало глобальным явлением, но все к этому идет. А потому, специалистам, отвечающим за корпоративную IT-инфраструктуру нужно к этому готовиться уже сейчас.

Давайте попробуем разобраться, что же такое BYOD, с какими трудностями может столкнуться компания и какие выгоды это может принести. Эксперты утверждают, что от использования собственных устройств гораздо больше плюсов, чем минусов. Сотрудникам нравится использовать принадлежащие им гаджеты, это улучшает микроклимат в коллективе и повышает производительность труда, так как они более привычны и удобны в использовании, чем те, которые может предложить организация. Кроме того, в теории, подобная тенденция помогает компании экономить деньги на покупке нового оборудования и существенно снизить расходы на IT-поддержке. Однако, как утверждает статистика, лишь немногие руководители разрешают приносить и использовать в работе собственные IT-устройства. Такая осторожность вызвана опасениями, что развитие BYOD потребует существенных расходов на обеспечение безопасности корпоративной сети, ведь сотрудник будет иметь доступ к конфиденциальной информации посредством личного устройства. Но это не нужно воспринимать, как головную боль, которую проносит BYOD. Ведь работники компаний годами имеют доступ к конфиденциальной информации, а наличие компакт дисков, USB-накопителей, камер на мобильных телефонах, электронной почты и банальной бумаги и ручки делали возможной утечку информации. Как бы там ни было, сотрудники будут приносить на работу свои собственные устройства даже без санкционирования со стороны руководства компании.Так что же делать в таком случае? Как говорится – возглавь то, что не можешь предотвратить! Определенные стандарты на аппаратное обеспечение удобны для IT-отдела компании, в то время как пользователи не всегда им рады. Требования к компьютерам зачастую различны даже внутри одного отдела, что уж говорить о разнице

между дизайнерами и менеджерами по продажам. Менеджер с дешевым и тяжелым ноутбуком, регулярно выезжающий на различные встречи и презентации, проигрывает в презентабельности своему конкуренту со стильным Sony VAIO или AppleMacBookAir. Да и те, кому приходится часто носить с собой ноутбук, готовы доплатить за меньший вес, привлекательный дизайн и другие немаловажные детали своего девайса. Благо зарплата многих менеджеров позволяет это сделать. Однако, это не означает, что стандартизированные рабочие места отошли в прошлое. Наоборот, они преобразились. Тот факт, что компьютер принадлежит пользователю, не препятствует установке на него принятых в компании ОС, включения устройства в домен и прочего. Естественно, будут свои трудности с любителями Mac OS и Linux, но и это решаемо.

Инициатива по поддержке данного тренда может исходить, как от самого сотрудника, так и от руководства (когда компания предлагает субсидии для покупки мобильного устройства, которое будет использовано в работе). В первую очередь, необходимо тщательно обдумать последствия стратегии BYOD и насколько это необходимо в вашей организации. Не стоит сразу отменять все корпоративные стандарты и предоставлять доступ всем и всюду. Ограничьтесь небольшой группой сотрудников. Не стоит применять политику BYOD к бухгалтерским подразделениям компании. Выявите предпочтения своих работников к возможным устройствам. Чтобы они сами хотели бы себе купить? И на основании этой информации можно будет сократить количество возможных устройств.

С устройствами разобрались, а как же быть с безопасностью корпоративной информации? С этим немного сложнее. Необходимо тщательно продумать такие важные аспекты:

- Четко объяснить сотрудникам, какая ответственность на них ложится, когда они получают непрерывный доступ к оборудованию и информации, используемой для решения рабочих задач.
- Какие минимальные требования к аппаратному обеспечению и операционной системе.
- Как, кто и сколько будет платить (аппаратное обеспечение, ПО, сервисная поддержка).
- Каковы политики удаленного доступа и безопасности.
- Уровень доступа к данным.

- Каковы способы безопасного хранения данных компании (возможно какие-то облачные сервисы).
- Как необходимо действовать в случае кражи или потери устройства.
- Что нужно делать в случае увольнения сотрудника.

Анализ ситуации – очень важный момент, на который стоит обратить внимание. Необходимо составить базу сотрудников и для каждого из них сделать пометку, пользуется ли он вычислительными мощностями компании (если «ДА», то чем именно) или же работает только со своим устройством. Подобная информация позволит отслеживать количество сотрудников пользующихся сервисом BYOD и прогнозировать долю таковых в будущем. Анализ тенденции позволит сделать прогноз того, как много, и какой именно техники понадобится компании с течением времени. Также, желательно проверить текущие лицензии на программное обеспечение, чтоб предоставить по необходимости доступ к лицензионному ПО, которое может понадобиться сотруднику для выполнения рабочих задач.

Такой сервис как BYOD позволяет сотруднику быть более мобильным и более оперативно реагировать на поставленные перед ним задачи. Это может быть очень полезно для работников, которым часто приходится ездить в командировки и личный ноутбук или iPad – это единственное средство получения доступа к необходимой рабочей информации.

Очень важно донести до сведения всех сотрудников требования к ним и обязанности компании в отношении их устройств. Понимание этой информации каждым работником организации нужно проверять с помощью аудитов и опросов, требуя ежегодно подписывать соответствующий документ. Компания должна предоставить все необходимое оборудование тем сотрудникам, которые не пользуются сервисом BYOD, а также тем, чьи устройства не позволяют решать им необходимые задачи. Поддерживающий персонал должен обладать всеми необходимыми средствами и навыками для поддержки сотен устройств, приносимых для работы в компании. Вообще, поддержка личных устройств сотрудников – это отдельный пункт, на который хотелось бы обратить ваше внимание.

Основная проблема заключается в том, что техническая служба компании не может оказывать помощь всем сотрудникам для всех устройств. И здесь должно быть четкое понимание границ оказания помощи сотрудниками технической поддержки. Например:

- поддержка устройства, при которой сотрудник сервисной службы предпринимает попытки для решения инцидента, понимая при этом, что

сбои связанные с BYOD-устройствами – это личные проблемы владельца данного устройства;

- ограничение поддержки по техническим областям, когда по некоторым технологиям поддержка осуществляется, а по некоторым нет;
- предоставление поддержки по контрактам, заключенным со сторонними сервисными организациями;
- обучение и проведение тренингов для сотрудников с целью познакомить их с наиболее часто возникающими неполадками и способами борьбы с ними.

Так что же мы должны понимать, принимая или не принимая в компании данный сервис? Основная мысль заключается в том, что принцип BYOD направлен на то, чтобы сделать сотрудников счастливыми, расширить их права и возможности, сделать более мобильными и повысить производительность труда. BYOD дает возможность привлекать, вовлекать и удерживать талантливых работников, ведь именно этого мы все и хотим.

Литература:

https://en.wikipedia.org/wiki/Bring_your_own_device

http://vido.com.ua/article/3112/byod-chietyrie-bukvy-sposobnyie-napughat-dazhie-krupnuiu-kompaniiu/

Свердлюк Богдан Игоревич
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ПЕРВЫМ ДЕЛОМ САМОЛЕТЫ, ИЛИ ТЕХНОЛОГИЯ ADS-B

С детства я люблю три вещи: самолеты, космос и мультфильмы. Сейчас хочу рассказать о одной из них - самолетах, а точнее каким образом они сообщают и определяют свое местоположение, сами получают информацию о воздушном трафике и экономят горючее

Одной из современных технологий передачи местоположения является ADS-B (это сокращение от Automatic Dependent Surveillance - Broadcast (автоматическое зависимое наблюдение в режиме радиовещания).
Система развертывается и поддерживается FAA (федеральным агенством гражданской авиации США). Она входит в программу под названием NextGen

Само название NextGen предвозвещает то, что это следующее поколение системы воздушного транспорта. Программа подразумевает переход от прошлой радиолокационной системы к единой системе на основании спутниковой навигации. Внедрение данной системы планируется на этапе с 2012 по 2025.

Что это?
Технология ADS-B позволяет наблюдать за самолетами как гражданской так и военной авиации. Это система, которая расширяет традиционные радарные системы. Технология ADS-B основана на передаче местоположения с помощью gps. Система, выстроенная с помощью этой технологии похожа на большую сеть, где самолеты выступают клиентами, а наземные станции точками доступа, по принципу “каждый видит каждого”, что позволяет предотвращать конфликтные ситуации, а также видеть весь трафик самолетов оснащенных оборудованием ADS-B. Это является одним из основных преимуществ, поскольку пилоты могут минимизировать временные интервалы и нагрузки на терминалы. Еще одним несомненным преимуществом является то, что радиус покрытия создаваемой сети наземным радаром ADS-B не имеет “дыр”. Это значит, что подобные станции могут располагаться где угодно. Стоит упомянуть, что станции данного типа намного дешевле в установке и использовании. Воздушные суда передают информацию о своем местоположении каждую секунду. Сравнительно с предшественником - радарной системой, которая обновлялся каждые 12 секунд это намного быстрее. (полный поворот антенны). С координатами самолет также передает скорость, номер, рейс, курс, статус и вертикальную скорость. В свою очередь на земле вся информация от ближайших самолетов объединяется с помощью компьютеров, выдается в наглядном виде диспетчерам и также ежесекундно широковещательно передается каждому, кто способен ее принять в радиусе обслуживания. Зачастую такой радиус составляет приблизительно 440 км. Информация с наземных станций комбинируется с информацией о погоде, графической информацией, сведениями о других судах, текстовой информации, например такой, как НОТАМ (оперативно распространяемая информация извещения).

Перспективы развития программы:
Уменьшение воздушных пробок
Существенное уменьшение затрат.
Сокращение потребления топлива
Уменьшение выбросов
Более точная информация маршрута для пилотов
Уменьшение времени задержек
Уплотнение воздушного трафика

Повышение безопасности и эффективности в воздухе, и на взлетно - посадочной полосе

Концепция ADS-B включает в себя четыре сервиса:
ADS-B - Естественно это сама система ADS-B в первую очередь. Ее суть состоит в том, что каждый самолет передает широковещательно сообщения с данными, которые принимают другие самолеты или наземные станции для диспетчерских потребностей.
ADS-R- Automatic Dependant Surveillance-Rebroadcast, система ретрансляции данных ADS-B для UAT (приемопередатчик универсального доступа) и обратно. Самолеты оборудованные UAT будут видеть самолеты оборудованные ADS-B и наоборот. UAT используется на старых самолетах и на легкомоторной авиации. Сервисы ADS-B и ADS-R относятся к сервисам "слежения и сопровождения" и отнесены FAA к критически важным для диспетчерских целей.
TIS-B
Traffic Information Services-Broadcast, или TIS-B, это часть ADS-B технологии, позволяющая самолетам, оборудованным приемниками ADS-B видеть летящие неподалеку другие самолеты не оборудованные системой ADS-B.
Координаты таких самолетов определяются наземными радарами и ретранслируются обратно в небо для всех самолетов в радиусе обслуживания.
FIS-B
Flight Information Services-Broadcast, или FIS-B, это часть ADS-B технологии, которая обеспечивает бесплатную информацию по погоде, временным ограничениям на полеты (temporary flight restrictions (TFRs)
Графические данные о погоде передаются только на 978 МГц
Вспомогательные программы Next Gen

Вспомогательные программы NextGen
Технологии управления воздушным движением (CATMT) представляет собой набор инструментов поддержки принятия решений и совместного использования данных персоналом управления воздушным движением. Это позволят более усовершенствовать среду совместной работы между наземными станциями и летчиками.
Передача данных (Data Comm) позволит диспетчерам передавать цифровые инструкции для пилотов. Точные визуальные сообщения, которые появляются на дисплее кабины могут взаимодействовать с бортовым компьютером воздушного судна. Тем самым уменьшая возможности ошибок, Comm Data вытесняет голосовую связь в качестве основного средства связи между диспетчерами и летным экипажем.

Национальная воздушная голосовая система (NVS) вытесняет прошлую FAA систему аналоговой голосовой связи. Это обеспечит большую гибкость движения.
NextGen Погода поможет уменьшить влияние погоды, предоставляя авиационные метеорологические данные. Это также понадобиться для разработки более надежных планов полетов, принимать более обоснованные решения.
Система управления информацией (SWIM) является сетевой структурой, которая будет передавать цифровую информацию в режиме реального времени.

Оборудование
Приемники ADS-B, установленные на борту другого самолета, в диспетчерском пункте или у вас дома, обеспечивают прием всех этих данных, а компьютер уже занимается обработкой и отображением их в удобной форме, например на карте.
ADS-B трансмиттеры (ADS-B OUT) - это когда воздушное судно передает ADS-B данные. Этот класс устройств может передавать ADS-B данные. Трансмиттеры также могут "пробуждать" FAA ADS-B наземные станции и переключать их в режим передачи трафика воздушным судам в зоне их действия. ADS-B устройства, способные передавать положение ВС и путь пролета должны быть сертифицированы FAA. Работает это оборудование на частоте 1090 MHz, или 978 MHz. Частота 1090MHz создана для полетов выше 5500 метров, в отличии от 978, где полет соответственно составляет высоту порядком ниже чем 5500 м,но требует установку дополнительного передатчика-радиоответчика (squawk code). Это решение дешевле, потому лучше подходят для легких негабаритных самолетов.
ADS-B приемники (ADS-B IN) это когда воздушное судно принимает данные FIS-B, TIS-B и другие. Эти устройства принимают данные ADS-B, но не могут передавать данные другим самолетам и наземным станциям.
Приемник получает как информацию о движении судов так и погодную информацию. В настоящее время FAA (федеральное управление гражданской авиации) ограничило работу системы. Самолет, оборудованный только ADS-B приемником, может и не "видеть" данные трафика, если другие самолеты в зоне обслуживания также не оборудованы ADS-B транспондерами и не передавали данные ADS-B.
Транспондер (transponder от transmitter-responder — передатчик-ответчик) — приемопередающее устройство, посылающее сигнал в ответ на принятый сигнал, например:
автоматическое устройство, принимающее, усиливающее и передающее далее сигнал на другой частоте;
автоматическое устройство, которое передает заранее заданное сообщение в ответ на заранее определенный принятый сигнал;

приёмопередатчик, который всегда создаёт ответный сигнал при правильном электронном запросе.

Погодная же информация всегда передается наземными станциями и всегда доступна для приема через ADS-B приемник в зоне действия. Для отображения ADS-B In данных необходим соответствующий дисплей. Это выглядит очевидным, но в реальности каждый производитель думает по своему.
ADS-B транспондеры - это когда, самолет принимает и передает данные напрямую от близлетящих воздушных судов. ADS-B транспондеры могут "пробуждать" FAA ADS-B наземные станции и переключать их в режим передачи трафика воздушным судам в зоне их действия. ADS-B устройства, способные передавать положение ВС и путь пролета должны быть сертифицированы FAA.

Отслеживание
Для отслеживания положения воздушного судна вы можете использовать собственный ADS-B приемник (к примеру microADS-B USB), и самим при желании передавать данные на сайты отслеживания воздушного транспорта, или воспользоваться данными предоставленными энтузиастами вашего региона на сайте. К примеру flightradar24.com, radarbox24.com, flightradar24.com и другими.
Цена данного радиоприемника начинается от 2000 грн. При этом пользователь получает доступ к определению данных судна, при оптимальных условиях, как и пилоты самолетов.
Использованные источники:

1. https://www.faa.gov/nextgen/works
2. http://forum.spotters.net.ua/viewtopic.php?f=1&t=842
3. http://www.ads-b.com/
4. www.flightradar24.com

Новіцька Наталія Вікторівна
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

БАЗОВІ СТАНЦІЇ

I. Постановка проблеми.

I.I. Що таке базова станція?

Базова станція - це системний комплекс приймально-передавальної апаратури, що здійснює централізоване обслуговування групи кінцевих абонентських

пристроїв.

I.II. Галузі використання.

- **В безпровідних мережах передачі даних**
  У безпровідних мережах передачіданихбазовастанція - цеприймачрадіосигналу, якийвиконує роль концентратора в дротовихлокальних мережах.
- **Професійний радіозв'язок**

У професійних системах радіозв'язку базова станція використовується як центральний вузол, що виконує диспетчерські функції в мережі мобільних радіостанцій з централізованою топологією, а також як передавач повідомлень в пейджинговому зв'язку. При цьому базова станція виступає в ролі одного з кінцевих вузлів в каналі зв'язку.

- **В безпровідній телефонії**

Базова станція в безпровідній телефонії зв'язується з мобільним безпровідним телефонним апаратом. При цьому сигнали від одного або декількох мобільних телефонів приймаються базовою станцією, яка передає ці виклики в наземні телефонні лінії.

- **У стільниковому зв'язку**

Базова станція стосовно до стільникового зв'язку - комплекс радіопередавачів, що здійснює зв'язок з кінцевим абонентським пристроєм – стільниковим телефоном.

Базові станції також застосовуються в стільниковому телебаченні, транкінговому зв'язку, мережах Wi-Fi та інших технологіях.

II. Мета.

Метою дослідження роботи базових станцій є вивчення принципів застосування, засобів, спільної взаємодії із Internet, телекомп'ютингом і віддаленим доступом до локальної мережі. Також виділення переваг по відношенню до показників аналогової телефонії.

III. Основні переваги використання базових станцій.

- **Спрощення логістики польових робіт.**
  Більше не потрібно встановлювати польову базову станцію і залишати персонал на її обслуговування, в тому числі, охорону. Скорочується кількість польових бригад, які потрібно транспортувати до місця робіт і назад. Простіше планувати час на виконання робіт, оскільки дані з постійно діючої базової станції доступні цілодобово.

- **Економія ресурсів.**
  Потрібна менша кількість польового персоналу, транспорту, ГНСС обладнання для виконання того ж обсягу робіт. Резервувати обладнання для використання як польових базових станцій більше не буде потрібно, а вже наявні супутникові приймачі можна використовувати більш ефективно, оптимізуючи інвестиції на придбання нового обладнання.
- **Гарантія точності результатів.**
  Всі визначення виконуються в системі координат вихідного пункту, місце розташування якого точно виміряна і постійно контролюється. Виключаються помилки установки польових приймачів над відомими точками.
  Важливо відзначити, що факт наявності постійно діючої базової станції дає переваги при виконанні будь-яких видів ГНСС зйомок.

Висновок.

В Україні, як і в усьому світі, спостерігається стрімке збільшення кількості інформаційних джерел — щодня будуються та реконструюються базові станції зв'язку, дообладнуються теле-радіопередавальні центри, об'єкти радіонавігації,станції супутникового зв'язку тощо.
Базова станція- це важлива складова ,яка забезпечує високу якість комунікацій!

Список використаних джерел.

Базова станція. [Електронний ресурс] – Режим доступу:https://uk.wikipedia.org/wiki/Базова_станція
ENTEL. [Електронний ресурс] – Режим доступу: http://www.ra.net.ua/entel/products/stations/base-stations/RP500/index.html
TNT TPI GNSS Network. [Електронний ресурс] – Режим доступу: http://www.tnt-tpi.com/послуги/мережа-базових-станцій

Дурман Володимир Володимирович
ДержавнийУніверситетТелекомунікацій
Факультет Телекомунікацій
м. Київ

АЛГОРИТМИ НАВКОЛО НАС

Люди щоденнокористуютьсярізноманітними правилами, інструкціями, рецептами тощо, щоскладаються з певноїпослідовності команд (вказівок). Деякі з них настількиувійшли до нашогожиття, що ми виконуємоїхмайже не замислюючись, інодікажуть, автоматично.

Такіпослідовності команд (вказівок) називають алгоритмами.
Алгоритм — цескінченнапослідовність команд (вказівок), щовизначає, якідії і в якому порядку потрібновиконати, щобдосягтипоставленої мети.
Двадцяте століття галузі техніки приніс людству багато великих досягнень: радіо, звукове кіно, телебачення, атомна енергія, космічні польоти, електронні обчислювальні машини — ось тільки найголовніші віхи, відомі кожному. Напевно, щонайменшевідомікібернетика, вірусологія, генетика.
Не всімвідомо, щонайбільшимдосягненням науки XX в. є теоріяалгоритмів — нова математичнадисципліна. Теоріяелектроннихобчислювальних машин, теорія і практика програмування не можекоштувати без неї. Математична і кібернетикапред'являютьїї у своїх прав. Але вона є самостійною наукою, яка готова служитивсім наук, і маєобличчя, свій предмет.
Багатохтовважає,щоінформатикапотрібнатільки для того, щобнавчитисяпрацювати на комп'ютерах, але це не так. Кожналюдинащоднязустрічається з безліччю задач віднайпростіших і добре відомих до дужескладних. Для багатьох задач існуютьвизначені правила (інструкції, команди), щопояснюютьвиконавцю, як розв'язуватидану проблему. Ці правила людинаможевивчитичизаздалегідьсформулювати сама в процесірозв'язуваннязадачі. Чим точнішеописані правила, тимшвидшелюдинаопанує ними і буде ефективнішеїхзастосовувати. У нашомужитті ми постійноскладаємоописдеякоїпослідовностідій для досягненнябажаного результату, тому поняття алгоритму не є для нас чимосьновим і незвичайним.
Кожний з нас використовуєсотнірізнихалгоритмів. Спробуйтезгадатидеякі з них (алгоритмивиконанняарифметичнихдій, розв'язування задач, прибиранняквартири, миття посуду, готуванняїжі — рецептитощо).

Для чоговивчатиалгоритми? По-перше, алгоритми є життєвонеобхіднимискладовими для рішення будь-яких задач з різноманітнихнапрямківкомп'ютерних наук. Алгоритмивідіграютьключову роль у сучасномурозвиткутехнологій. Тут можназгадатитакірозповсюдженізадачі, як:
розв'язанняматематичнихрівняньрізноїскладності,
знаходженнядобуткуматриць,
оберненихматриць;знаходженняоптимальнихшляхівтранспортуваннятоварів та людей;
знаходженняоптимальнихваріантіврозподіленняресурсівміжрізнимивузлами (виробниками, верстатами, працівниками, процесорамитощо); знаходження в геноміпослідовностей, якіспівпадають;пошукінформації в глобальніймережіІнтернет; прийняттяфінансовихрішень в електроннійкомерції;

обробка та аналізаудіо та відеоінформації. Цей список можнапродовжувати й продовжувати і, власнокажучи, майженеможливознайтитакугалузькомп’ютерних наук та інформатики, де б не використовувалисьтіабоіншіалгоритми. По-друге, якісні та ефективніалгоритмиможутьбутикаталізаторамипроривів у галузях, які є на перший погляд далекими відкомп’ютерних наук (квантовамеханіка, економіка та фінанси, теоріяеволюції). І, по-третє, вивченняалгоритмівцетакожнеймовірноцікавийпроцес, якийрозвиваєнашіматематичніздібності та логічнемислення.

Звичайно, не забороняється математику вивчатианалітичнутеоріюалгоритмів без того, щобзамислюватися про реальнийсвіт, хочаце і не можнасхвалити. Точно так само не забороняється, вивчаючилогічнутеоріюалгоритмів, вважати, що слова є описамиреальнихоб'єктів.Алелогічнатеоріяалгоритмівнавіть не натякає на який-небудьспосібописуоб'єктів у виглядіслів, тоді як аналітичнатеоріятакінатякиробить. Наприклад, для описуоб'єктівнапрошуєтьсязастосуванняприйому, званого структуризацією, якийпередбачаєрозчленуванняоб'єкта на складовічастини - більшпростіоб'єкти, до якихзновузастосовується той же прийом, і так до тих пір, поки не буде отриманаконструкція, побудована з допомогоюзв'язків з таких простихоб'єктів, які ми вжевміємопредставляти у виглядісимвольнихконструкцій.Точно так само складніопераціїконструюються з натуральних шляхом побудовиалгоритмів.

Література:

1.http://bukvar.su/informatika_programmirovanie/173594-Algoritmy-vokrug-nas.html

2.http://formula.co.ua/blog/alhorytmy-ta-jih-vlastyvosti/

3.http://oim.asu.kpi.ua/files/TA/01_Algorithms_and_calculations.pdf

4.http://ua-referat.com/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%B8_%D0%BD%D0%B0%D0%B2%D0%BA%D0%BE%D0%BB%D0%BE_%D0%BD%D0%B0%D1%81

5.https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC

Дурман Володимир Володимирович
ДержавнийУніверситетТелекомунікацій
Факультет Телекомунікацій
м. Київ

АЛГОРИТМИ НАВКОЛО НАС

1.Поняття алгоритму

Повсякденне життя кожної людини полягає у вирішенні величезної кількості завдань різної складності на роботі або під час навчання. Деякі завдання є настільки простими, що при їх виконанні ми робимо певні дії автоматично, навіть не замислюючись. Рішення будь-якої задачі, навіть найпростішої, як правило, здійснюється послідовно за кілька кроків. Такого роду послідовність при вирішенні завдань називається алгоритмом.

Саме **поняття «алгоритм»** виникло із назви латинського перекладу книжки арабського математика IX століття Аль-Хорезми «AlgoritmidenumeroIndoru», що можна перекласти як «Трактат Аль-Хорезми про арифметичне мистецтво індусів». Упорядкування алгоритмів і питання існування є предметом серйозних математичних досліджень.

У 1843 р. Ада Лавлейс описала алгоритм обчислення чисел Бернуллі на аналітичній машині Беббіджа. Цей алгоритм визнано першою програмою, спеціально реалізованою, щоб виконуватися на ЕОМ, і через це його розробницю вважають першим програмістом, дарма що машина Беббіджа не була сконструйована за життя Ади.

З 1930-х рр. починається бурхливий розвиток галузі дослідження алгоритмів та становлення інформатики в її сучасному вигляді. В 1935 році Стівен Кліні розробив перше формулювання теорії рекурсії та показав еквівалентність розробленої системи частково рекурсивним функціям. В 1936 році незалежно були опубліковані роботи Алана Тюринга та Еміля Поста, в яких наведено схожі системи для визначення поняття алгоритму. А вже в 1937 році було доведено еквівалентність різних визначень.

Машина Тюринга пропонувала конструкцію, придатну для автоматичної інтерпретації. Побудована під впливом Алана Тюринга у Великобританії обчислювальна система ACE (завершена в 1950 році), та системи, побудовані за архітектурою фон Неймана в США та в інших країнах (в СРСР — МЕСМ, розроблена в 1950 році в Інституті електротехніки АН УРСРгрупою вчених під керівництвом Сергія Лебедєва), були першими універсальними обчислювальними пристроями, які повністю задовольняли вимоги обчислюваності.

Протягом 1935-1960 років було розроблено численні ідеї та технології, які лягли в основу сучасної інформатики.

Надалі алгоритмом почали називати**точне розпорядження, або послідовність дій, що забезпечує отримання необхідного результату із вихіднихданих.**
Алгоритм призначений до виконання його людиною чи автоматичним пристроєм. Створення алгоритму, навіть найпростішого, - процес творчий. Він доступний виключно для живих істот. Інша річ - реалізація вже наявного алгоритму. Її можна доручити суб'єкту чи об'єкту, який зобов'язаний вникати у суть справи, а можливо, і здатний її зрозуміти. Такий суб'єкт чи об'єкт прийнято називати**формальним виконавцем.** Прикладом формального виконавця може бути пральна машина-автомат, яка точно виконує належні їй дії, навіть коли ви забули покласти у неї порошок. Людина також може стати в ролі формального виконавця, та в першу чергу формальними виконавцями стають різні автоматичні пристрої, комп'ютер зокрема. **Кожен алгоритм створюється для цілком конкретного виконавця.** Ті дії, що може здійснювати виконавець, називаються **його допустимими діями**. Сукупність допустимих дій утворює **систему команд виконавця.** Алгоритм мусить мати ті дії, які припустимі для даного виконавця.
Об'єкти, з яких виконавець може виконувати дії, утворюють так зване **середовище виконавця.**

2. Як виникають алгоритми

Одним з джерел створення алгоритмів є практика, яка надає нам дві основні можливості: спостереження і експеримент (а також будь-які їх комбінації).
Об'єктом спостереження може бути будь-яка жива істота, яка вміє вирішувати будь-яке з виникаючих перед нею завдань. Описуючи його дії, аналізуючи їх залежність від мінливих обставин, можна отримати алгоритм для розв'язання даного завдання.
У більш складному випадку об'єктом спостереження може бути колектив спільно діючих живих істот.
У ще більш складних випадках спостерігають будь-який процес, що протікає в неживій природі, організмі або в суспільстві, вивчають вплив на нього різних факторів, в кінці кінців може бути отриманий алгоритм управління цим процесом (який буде ефективним, якщо існує реальна можливість змінювати визначають процес- фактори). Алгоритми, отримані таким чином (у тому числі і що імітують), прийнято називати *емпіричними.* До їх числа відносяться алгоритми приготування їжі, приготування ліків, тощо.
Алгоритми, що призводять до вирішення цікавих для нас задач, іноді можна отри-мати експериментально, підбираючи дії, що призводять до бажаного результату. Їх ми не будемо виділяти в окрему групу і умовно віднесемо до емпіричних.
В якості **другого джерела** слід вказати наукову теорію, з основних положень та встановлених фактів якій алгоритми в деяких випадках можуть бути

виведені. До цієї групи належить наприклад алгоритм додавання десяткових дробів.

Третім джерелом нових алгоритмів може бути сукупність вже накопичених. Виявляється, за допомогою спеціальних прийомів з наявних алгоритмів можна отримувати нові.

Нарешті, **четвертим джерелом** алгоритмів може бути винахідливість їх розробника.

Як би не був отриманий алгоритм, він повинен бути обґрунтований; це означає, що якщо алгоритм створений для вирішення певної задачі, то необхідна впевненість в тому, що для всіх вихідних даних, для яких це завдання може бути вирішене, алгоритм дозволяє отримати рішення і ні для яких вихідних даних не дає неправиль-ного результату. Це називається *коректністю*алгоритму.

Повна впевненість в коректності алгоритму виникає лише в тому випадку, коли отримані з його допомогою результати не лише підтверджуються експериментально, але й узгоджуються з усіма іншими накопиченими та об'єднаними в наукову теорію фактами цієї галузі науки або техніки.

Створення алгоритму вирішення завдань будь-якого типу, його уявлення виконав-цем в зручній йому формі – це творчий акт. Алгоритм можна представити у різний спосіб: на розмовній природній мові; мовою блок-схем; мовою програмування. Вибір й розробка алгоритму із чисельних методів виконання завдання мають найважливіше значення на шляху успішної роботи над програмою. Старанно опрацьоване виконання завдання – необхідна умова ефективної роботи із складання алгоритму.

Поширеним критерієм оцінки алгоритмів є *час роботи* та *порядок зростання тривалості* роботи в залежності від обсягу вхідних даних

3. Поняття алгоритму в інтуїтивному розумінні

Роз'яснимо поняття алгоритму в інтуїтивному розумінні на ряді прикладів. До числа алгоритмів не відносяться правила,які що-небудь забороняють, наприклад: «Вхід стороннім заборонено», «Не палити», «В'їзд заборонений» (зображується відомим кожному водієві автомобіля знаком «цеглина»).Не належать до них і правила, які що-небудь дозволяють, такі як «Дозволена стоянка автотранспорту», «Вхід», «Місце для куріння".А ось - «Йдучи, гасіть світло», «Йти ліворуч, стояти справа» (на ескалаторі в метрополітені) - це вже алгоритми, хоча і дуже примітивні. Потрібно відзначити одну особливість алгоритму: дискретний **характер процесу**, що визначається самим алгоритмом.Правило «Під час руху по тротуару дотримуйся правого боку», хоча і є приписом, але має безперервний характер і тому не відноситься до числа алгоритмів.

Подібні правила дуже численні й нерідко мають велике значення в нашому житті. Народжуючись, людина відразу потрапляє в «гущу» алгоритмів.

Алгоритми грають роль не тільки в житті людей. Наприклад:

«Кожне цуценя слід годувати окремо від інших, інакше сильніші і активніші будуть з'їдати велику порцію».
В останньому правилі фраза «... інакше сильніші і активніші будуть з'їдати велику порцію» до самого правила не відноситься. Такі фрази називають *коментарями.* Їх відкидання на сенс правила не впливає.
Цікаві приклади алгоритмів представляють широко відомі рецепти, за якими в аптеках готують і видають ліки. Лише дуже досвідчені лікарі складають кожен раз індивідуальний рецепт, в більшості ж випадків його виписують із спеціального довідника.
Від точності виконання подібного алгоритму часом залежить життя людини.
А ось за столом сидить школяр. Чим він зайнятий? За його словами, він готує уроки. Яке до цього мають відношення алгоритми? Виявляється - велике. Він вирішує приклади з арифметики, складає десяткові дроби. Запитайте його, як він це робить, і він відповість:
«Спершу я одну дріб підписую під інший так, щоб однойменні розряди стояли один під одним. Якщо в одному з чисел не вистачає ліворуч або праворуч цифр, я доповнюю його нулями.
Кількість одиниць в отриманому результаті записую в однойменний розряд суми, а число десятків приймаю за перенесення в наступний розряд.
Найперше перенесення (в молодший розряд) завжди вважається рівним нулю. А якщо в старшому розряді виникає перенесення, то перед початком обох чисел потрібно приписати по нулю. Процес закінчується тоді, коли вичерпуються всі розряди доданків ».
Це - алгоритм. Може бути, учень і не зуміє його викласти так, як тут написано, і обмежиться більш лаконічним «складаю числа», але він його звичайно виконує.
Не тільки діти, а й дорослі більшу частину свого часу витрачають на виконання алгоритмів. Багато інструкції та накази, які визначають наші дії на роботі, - це алгоритми. Навіть закінчивши роботу і бажаючи відпочити, ми постійно стикаємося з ними.
Усюди алгоритми. Вони оточують нас, переплітаються, проникають один в одного; кроку не можна ступити, не наражаючись на них. Але як разюче відрізняються «алгоритмічні джунглі» від справжніх, в яких густі сплутані рослини стискаючи нас, чіпко тримають в полоні. Дивним чином алгоритми не пов'язують нас, а ведуть найнадійнішими шляхами до вирішення найскладніших проблем.

4. Нумерація алгоритмів

Нумерація алгоритмів відіграє важливу роль в їхньому досліджені та аналізі.

Оскільки будь-який алгоритм можна задати у вигляді скінченного слова (представити у вигляді скінченної послідовності символів деякого алфавіту), а множина всіх скінченних слів у скінченному алфавіті зліченна, то множина всіх алгоритмів також зліченна. Це означає існування взаємно однозначного відображення між множиною натуральних чисел та множиною алгоритмів, тобто можливість присвоїти кожному алгоритму номер.

Нумерація алгоритмів є, водночас, і нумерацією всіх алгоритмічно обчислюваних функцій, при чому, будь-яка функція може мати нескінченну кількість номерів.

Існування нумерації дозволяє працювати з алгоритмами так само, як з числами. Особливо корисна нумерація в дослідженні алгоритмів, що працюють з іншими алгоритмами.

5. Властивості алгоритмів

Алгоритми мають ряд важливих властивостей:

Скінченність

алгоритм має завжди завершуватись після виконання скінченної кількості кроків. Процедуру, яка має решту характеристик алгоритму, без, можливо, скінченності, називають *методом обчислень*.

Дискретність

процес, що визначається алгоритмом, можна розчленувати (розділити) на окремі елементарні етапи (кроки), кожен з яких називається кроком алгоритмічного процесу чи алгоритму.

Визначеність

кожен крок алгоритму має бути точно визначений. Дії, які необхідно здійснити, повинні бути чітко та недвозначно визначені для кожного можливого випадку.

Вхідні дані

алгоритм має деяку кількість (можливо, нульову) вхідних даних, тобто, величин, заданих до початку його роботи або значення яких визначають під час роботи алгоритму.

Вихідні дані

алгоритм має одне або декілька вихідних даних, тобто, величин, що мають досить визначений зв'язок із вхідними даними.

Ефективність

алгоритм вважають ефективним, якщо всі його оператори досить прості для того, аби їх можна було точно виконати за скінченний проміжок часу з допомогою олівця та аркушу паперу.

Масовість

властивість алгоритму, яка полягає в тому, що алгоритм повинен забезпечувати розв'язання будь-якої задачі з класу однотипних задач за будь-якими вхідними даними, що належать до області застосування алгоритму.

6. Висновки

Тепер ми вже можемо точніше сказати, що таке алгоритм. *Алгоритм* - це правило, сформульоване на деякій мові і визначає процес переробки допустимих вихідних даних в шукані результати. Припустимими вихідними даними для цього правила є пропозиції мови вихідних даних. Правило характеризується зрозумілістю для виконавця, масовістю і визначеністю.

У наведених вище прикладах алгоритми породжують чітко видимі алгоритмічні процеси, кожен крок яких дуже простий. Якщо алгоритм до яких-небудь допустимих вихідних даних непридатний, то алгоритмічний процес може для цих вихідних даних або тривати необмежено (бути нескінченним), або безрезультатно обриватися.

Тепер у «алгоритмічних джунглях» вже можна в якійсь мірі орієнтуватися. Ми розуміємо, що таке алгоритм і навіщо він потрібний.

На першому етапі свого розвитку теорія алгоритмів не прагнула дати досить широкого визначення алгоритму, але співвідношення між формальним і інтуїтивним поняттями алгоритму завжди було в центрі уваги вчених.

7. Література

1.http://ua-referat.com/
2.http://bukvar.su/informatika_programmirovanie/page,3,173594-Algoritmy-vokrug-nas.html
3.http://distance.edu.vn.ua/metodic/pascal/4.htm
4.http://lits.ua/lc-school/algorithms
5.http://formula.co.ua/blog/alhorytmy-ta-jih-vlastyvosti/

Лугінець Вадим Віталійович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

АНТИВІРУСНИЙ ЗАХИСТ СИСТЕМИ КОМП'ЮТЕРА

Згідно даним дослідження Українського Антивірусного Центру (http://www.unasoft.com.ua/), вірогідність наявності вірусів в системі комп'ютера, що позбавлений захисних програм, складає 99%. Навіть у тих випадках, коли дія вірусів непомітна і не впливає на ефективність роботи системи, треба профілактично сканувати обладнання, бо активація деяких вірусів пов'язана з певним терміном (показником дати або часу). Коли комп'ютер не приєднаний до Інтернету і антивірусний захист здається користувачеві зайвим, треба пам'ятати, що джерелом вірусів може стати

змінний накопичувач інформації чи компакт диск невідомого виробника. Результатом такої необачливості може стати некоректна робота обладнання або втрата програми та інформації, все залежить від того, який вірус ви «підхопили». Про типи вірусів та інші шкідливі програми можна прочитати у стислому і неважкому для розуміння огляді Олега Сича (http://www.getinfo.ru/article371.html).

Антивірусний захист може забезпечуватись:

встановленнямнакомп'ютерповноїверсіїантивірусноїпрограми, якізапускаютьсяпризавантаженнісистемиіавтоматичнопроводятьскануваннярозділивжорсткогодиску, оперативноїпам'яті, змінних носіїв, електронної пошти, сторінокІнтернетутаін. безпосередньоупроцесіроботи, атакожавтоматичночерезІнтернетоновлюютьсвоїантивірусні бази. Недоліком цих програм є досить висока вартість ліцензованого продукту та відбір потужності комп'ютеру і, як наслідок, зниження швидкості його роботи.

періодичним скануванням системи спеціальними версіями антивірусних програм. Виробники випускають оновлені версії таких програм щотижня. Деякі програми потребують інсталяції, а після сканування самовидаляються. Інші – запускаються з файлу і їх потрібно оновлювати чи видаляти вручну, або безпосередньо з Інтернету.

Типантивірусноїпрограмивизначаєтьсязалежновідпотужностікомп'ютеру татим, наскількичастовінпідключаєтьсядозмінних носіївінформаціїчиІнтернету. Не останнім фактором у виборі програми є зручний інтерфейс, але тут все залежить від вимог користувача.

НайбільшудовіруукористувачівмаютьпрограмамизахистуАнтивірусКаспе рського (йогопробнуверсіюможнабезкоштовнозавантажитизсайтувиробниказаадресою: http://www.kaspersky-antivirus.com.ua/servis/download.html); Dr.Web безкоштовнонадаєсвоїмкористувачампробнуверсіюповногопродуктутапрограму длясканування системи Dr.Web CureIt, якуможназавантажитизісторінки http://www.freedrweb.com/cureit/.

Треба виокремити новий вітчизняний антивірусний продукт, вдосконалення якого ще продовжується виробниками, але вже визнаного користувачами. Зілля (Zillya) – повна версія першого українського антивірусніку, який зараз знаходиться у вільному доступі (http://zillya.com/) і надає користувачеві повний набір сервісів безкоштовно.

Безкоштовні версії антивірусних програм можна завантажити з сайтів виробників, а можна скористатися спеціальними Інтернет-бібліотеками (наприклад, http://biblprog.org.ua/ru/), які надають можливість порівняти програми за описом і вибирати необхідний ресурс. Нижче наведено перелік найпопулярніших продуктів.

 Avira AntiVir Personal

 Panda Cloud Antivirus

 AVG Anti-Virus Free

 Zillya

 PC Tools Aantivirus Free

 Dr.Web_Cureit

 Kaspersky virus removal tool

 Avast! Free Antivirus

 Bitdefender

В умовах, коли більшість навчальні закладів користуються не найпотужнішими комп'ютерами і такі ж комп'ютери встановлені вдома у вчителів, особливе значення набуває захист періодичним тестуванням системи. Покращити якість сканування системи комп'ютера на наявність вірусів можна, якщо провести його у безпечному режимі. При роботі системи у стандартному режимі автоматично запускається ціла низка допоміжних програм-утиліт під які, до речі, і маскується частина вірусів. Безпечний режим роботи автоматично бере до виконання тільки систему «життєзабезпечення» комп'ютера та ті програми, виконання яких призначає сам користувач. Наведемо алгоритм такого сканування:

Відключити систему відновлення системи, виконавши наступну послідовність дій: відкрити контекстне меню папки **Мій комп'ютер >** обрати **Властивості > відкрити** вкладку **Відновлення системи >** встановити прапорець навпроти призначення **Вимикнути відновлення системи на всіх дисках**> підтвердити свої дії, натиснувши **«ОК».**

Перезавантажити комп'ютер, натиснувши на клавіатурі клавішу **F8** після тестування Біос, але перед початком запуску Windows.

У меню, що відкриється, обрати **Безпечний режим**. Далі підтвердити бажання завантаження Windows. У безпечному режимі робочій стіл виглядає трохи інакше: відсутній фоновий малюнок, у кожному куті екрану вказано, що машина працює у безпечному режимі.

Запустити антивірусну програму і розпочати тестування.

Після завершення тестування перезавантажити комп'ютер та відновити Функцію **Відновлення системи.**

Використані джерела:
[http://ittexnoall.com/index.php/programki/108-antivirusnij-zakhist-komp-yutera.html];
[http://www.getinfo.ru/article371.html].

Лугінець Вадим Віталійович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

СОВРЕМЕННЫЕ ТИПЫ КОМПЬЮТЕРНЫХ ВИРУСОВ И ДРУГИХ ВРЕДОНОСНЫХ ПРОГРАММ

В настоящее время все мы можем наблюдать повальную информатизацию нашего общества. Там, где ещё вчера работа велась дедовским методом (кипы бумаг, счёты, калькуляторы), сегодня всё чаще и чаще мы видим компьютеры. Количество компьютеров растёт, их объединяют в локальные сети и со временем, как правило, подключают к глобальной сети Интернет (или, по крайней мере, к некоторым её сервисам, таким как электронная почта). А вместе с тем люди, которых поставили перед фактом, что отныне они должны делать свою работу с использованием передовых технологий вычислительной техники, не имеют ни малейшего опыта работы с компьютерами. И если непосредственную работу они хоть как-то худо-бедно учатся делать (запоминая на какие кнопочки, и в каком порядке надо нажимать), то обо всех подстерегающих их опасностях не имеют ни малейшего представления.

Именно отсюда и все наши беды: тысячи пользователей, которых принудительно посадили за клавиатуру, не научив толком как ею пользоваться. Ну что, к примеру, может знать о вирусах или уязвимостях Internet Explorer женщина-бухгалтер подпенсионного возраста, которая всю жизнь пользовалась древнейшим компьютером - счётами.

За долгие годы работы в сфере антивирусной безопасности специалистами Украинского Антивирусного Центра (www.unasoft.com.ua) выведена закономерность: если организацией используются компьютеры (не обязательно даже объединённые в локальную сеть), активно используется Интернет (или хотя бы электронная почта) и не применяются антивирусные средства (или не обновляются базы антивирусных продуктов) то с 99%-ой уверенностью можно сказать - в организации есть вирусы. И пусть до поры до времени они себя никак не проявляют, но это бомба. И рано или поздно эта бомба взорвётся.

Вообще в последние 2 года наибольшим источником компьютерных вирусов является именно глобальная сеть Интернет. Из нее к пользователям попадают минимум 95% всех вредоносных программ.

По определению вирусами являются программы, которые имеют возможность создавать свои копии, которые в свою очередь сохраняют способность к размножению (размножение - главное свойство вируса). Но это определение вируса в узком смысле этого слова. В широком же смысле слова мы называем вирусами как собственно сами вирусы, так и: Internet-черви, сетевые черви, троянские программы, утилиты скрытого администрирования.

Вирусы

Сами вирусы в узком смысле этого слова ранее были наиболее массовым типом вредоносных программ. Наиболее распространённые из них нынче: Win95.CIH, Win32.Funlove, Win32.Elkern. Но сейчас они потеряли былую "популярность". Связано это, прежде всего с тем, что переносятся такие вирусы с компьютера на компьютер через исполняемые файлы. Нынче же пользователи всё реже и реже переписывают друг у друга программы. Чаще меняются компакт дисками или ссылками всё в той же глобальной сети. Хотя естественно полностью этот класс вредоносных программ не вымер, и время от времени мы слышим о заражении компьютеров всё тем же "Чернобылем" (WinCIH) или ещё чем-то до боли знакомым.

Кроме того существует огромное наследие: десятки тысяч вирусов, написанных для операционной системы MS DOS. Большинство этих вирусов не могут существовать в современных версиях Windows, и тем не менее остаётся угроза, что кто то случайно или намеренно активизирует на компьютере вирус, нанеся тем самым непоправимый вред.

Internet-черви

Самым распространённым типом вирусов в последние два года являются Интернет черви. Именно они представляют главную угрозу для всех пользователей глобальной сети. Почти все Интернет черви - это почтовые черви, и лишь малая доля - это непочтовые черви, применяющие уязвимости программного обеспечения (как правило, серверного). Примеры непочтовых Internet-червей: IIS-Worm.CodeRed, IIS-Worm.CodeBlue, Worm.SQL.Helkern.

Почтовые черви можно делить на подклассы по-разному, но для конечного пользователя они делятся на два основных класса:

Черви, которые запускаются сами (без ведома пользователя);

Черви, которые активизируются, только если пользователь сохранит присоединённый к письму файл и запустит его.

К первому типу относятся черви, которые используют уязвимости (ошибки) почтовых клиентов. Чаще всего такие ошибки находятся в почтовом клиенте Outlook, а вернее даже не в нём, а в Интернет браузере Internet Explorer. Дело в том, что MS Outlook создаёт письмо в виде HTML страницы и при отображении этих страниц он использует функции браузера Internet Explorer.

Наиболее распространённая уязвимость, применяемая червями, ошибка IFRAME. Применяя соответствующий код, вирус имеет возможность при просмотре письма автоматически сохранить присоединённый к письму файл на диск и запустить его. Самое обидное то, что данная уязвимость обнаружена более двух лет назад. Тогда же компанией Microsoft выпущены заплатки для всех версий браузера Internet Explorer, исправляющие эту ошибку. И, тем не менее, черви, применяющие данную уязвимость, по-прежнему являются наиболее распространёнными (I-Worm.Klez, I-Worm.Avron, I-Worm.Frethem, I-Worm.Aliz).

Почтовые черви второго типа рассчитаны на то, что пользователь, по каким то соображениям сам запустит программу, присоединённую к письму. Для того чтобы подтолкнуть пользователя к запуску инфицированного файла авторами червей применяются различные психологические ходы. Самый распространённый приём - выдать зараженный файл, за какой то важный документ, картинку или полезную программку (I-Worm.LovGate создаёт ответы на письма, содержащиеся в почтовой базе; I-Worm.Ganda маскируется под информацию о боевых действиях в Ираке). Практически всегда червями применяются "двойные расширения". В этом случае присоединённый файл имеет имя вроде: "Doc1.doc.pif", "pict.jpg.com". Данный принцип рассчитан на то, что почтовые клиенты не отображают полное имя файла (если оно слишком длинное), и пользователь не увидит второго расширения, которое и является "реальным". То есть пользователь думает, что файл является документом или картинкой, а тот на самом деле является исполняемым файлом с расширением вроде: EXE, COM, PIF, SCR, BAT, CMD и т.п. Если такой файл "открыть", то тело червя активизируется.

Кроме основной функции, размножения, черви почти всегда несут в себе и боевую нагрузку. Действительно, зачем писать червя и выпускать его "в свет", предварительно не заложив бомбу. Вложенные функции чрезвычайно разнообразны. Так, например, очень часто почтовые черви призваны для того, чтобы установить на зараженный компьютер троянскую программу или утилиту скрытого администрирования и сообщить адрес компьютера творцу червя. Не редко просто уничтожают информацию или просто делают невозможной дальнейшую работу на компьютере. Так червь I-Worm.Magistr выполнял те же действия, что и печально-известный WinCIH - стирал содержимое FLASH BIOS и затирал мусорными данными информацию на жёстком диске.

В любом случае, независимо от наличия или отсутствия вредоносных функций и их "опасности" почтовые черви вредны уже только потому, что они существуют. Это связано с тем, что при размножении они загружают каналы связи и нередко настолько, что полностью парализуют работу человека или целой организации.

Макро-вирусы

Вторыми по распространённости в диком виде являются макро-вирусы. Данные вирусы являются макросами, хранящимися во внешних файлах программного обеспечения (документах Microsoft Office, Autocad, CorelDRAW и пр.) и при открытии документа исполняются внутренними интерпретаторами данных программ. Широкое распространение они получили благодаря огромным возможностям интерпретатора языка Visual Basic, интегрированного в Microsoft Office.

Излюбленным местом обитания этих вирусов являются офисы с большим документооборотом. В таких организациях людям, работающим за компьютерами (секретари, бухгалтеры, операторы ЭВМ) некогда заниматься

такими мелочами как компьютерные вирусы. Документы лихо переносятся с компьютера на компьютер, без какого либо контроля (особенно при наличии локальной сети).

К сожалению, людям свойственно не воспринимать всерьёз макровирусы, а напрасно. На самом деле макрос, написанный на языке VBA и интегрированный в документ того же Word или Excel, обладает всеми теми же возможностями, что и обычное приложение. Он может отформатировать Ваш винчестер или просто удалить информацию, украсть какие то файлы или пароли и отправить их по электронной почте. Фактически вирусы этого класса способны парализовать работу целого офиса, а то даже и не одного.

Опасность макровирусов заключается ещё и в том, что распространяется вирус целиком в исходном тексте. Если человек, к которому попал вирус, более-менее умеет писать на Visual Basic, то он без труда сможет модифицировать вирус, вложить в него свои функции и сделать его невидимым для антивирусов. Не забывайте, что авторы вирусов пользуются теми же антивирусными программами и модифицируют свои вирусы до тех пор, пока те не перестают детектироваться антивирусами. Фактически, таким образом, рождаются новые модификации уже известных вирусов, но для того, чтобы данный вирус обнаруживался антивирусом, он сначала должен попасть в антивирусную лабораторию и только после этого будут добавлены функции детектирования и обезвреживания новой модификации. Так специалистам Украинского Антивирусного Центра известно более 100 модификаций вируса Macro.Word97.Thus, более 200 модификаций Macro.Word97.Marker и более 50 модификаций Macro.Word97.Ethan (здесь речь идёт о модификациях, значительно отличающихся друг от друга, что требует добавления дополнительных модулей детектирования и лечения данных модификаций вирусов).

Троянские программы и утилиты скрытого администрирования

Следующими по распространённости являются Trojan и Backdoor программы. Отличие этих двух типов программ заключается в том, что троянская программа выполняет активные действия (уничтожение данных, сбор данных и отправка через Internet, выполнение каких либо действий в определённое время), в то время как Backdoor-программы открывают удалённый доступ к компьютеру и ожидают команды злоумышленника. Для простоты будем называть оба этих класса троянскими программами.

Главное отличие "троянов" от всех перечисленных выше творений человеческого разума является то, что троянские программы не размножаются сами. Они единоразово устанавливаются на компьютер и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы по какой либо причине) выполняет свои функции. При этом троянский конь не может самостоятельно переместиться с одного компьютера в локальной сети на другой.

Так почему же Трояны так распространены. Причина таится именно в том, что они максимально "полезны" и незаметны. Часто они являются спутниками сетевых или почтовых червей. Так, почтовый червь I-Worm.LovGate при попадании на компьютер устанавливает в систему backdoor модуль, открывающий доступ к компьютеру по TCP/IP и отправляет разработчику червя письмо, в котором указывается имя пользователя, имя компьютера и сетевой адрес зараженного компьютера.

Все троянские программы можно разделить на три основных класса по выполняемым действиям:

Логические (временные) бомбы - программы, различными методами удаляющие/модифицирующие информацию в определённое время, либо по какому то условию.

Шпионы - собирающие информацию (имена, пароли, нажатия на клавиши) и складирующие её определённым образом, а не редко и отправляющие собранные данные по электронной почте или другим методом.

Собственно ***BackDoor программы*** - удалённое управление компьютером или получение команд от злоумышленника (через локальную/глобальную сеть, по электронной почте, в файлах, от других приложений, например тех же червей или вирусов).

Одинаково опасны все три типа программ. Каждый из них способен либо уничтожить данные, либо украсть ценную информацию (хотя бы те же имена и пароли доступа к различным ресурсам).

Стоит отметить, что многие троянские программы постоянно обновляются, выходят всё новые и новые модификации. Учитывая то, что троянская программа не может попасть к вам случайно, злоумышленник старательно выбирает: какой бы троян вам установить. Очень велика вероятность того, что он пойдёт в Интернет и выкачает что то свеженькое. Именно поэтому необходимо регулярно обновлять базы антивирусного продукта. Так обновления для системы антивирусной защиты "Украинский Национальный Антивирус" (UNA) выходят каждый день. И если вы активно пользуетесь Интернетом, рекомендуем обновлять антивирус минимум раз в неделю (хотя конечно идеально было бы обновляться каждый день).

В завершение хотелось бы сказать: процесс развития вирусов и антивирусов - это постоянная война технологий. Регулярно в вирусах реализовываются оригинальные идеи, что требует адекватных действий от разработчиков антивирусного ПО. Поэтому рядовому пользователю рекомендуется следить за новостями на сайтах антивирусных компаний и прислушиваться к советам специалистов по информационной безопасности о необходимости обновления программного обеспечения (не только антивирусного) или выполнении специфических действий по улучшению защищённости ПК.

Використані джерела:
[http://ittexnoall.com/index.php/programki/108-antivirusnij-zakhist-komp-yutera.html];
[http://www.getinfo.ru/article371.html].

Бут Олександр Дмитрович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ЩО ТАКЕ 5G МЕРЕЖА?
КОЛИ 5G З'ЯВИТЬСЯ В УКРАЇНІ?

Настало століття інновацій і високих технологій і у людини з'явилося багато додаткових можливостей. Гаджети з безліччю функцій, легкі комп'ютери і багато іншого.

У всіх цих технологій є одна важлива функція, яка їх об'єднує - це доступ в Інтернет.

Всі сучасні пристрої, які мають доступ в Інтернет, зараз використовують 3G і 4G (LTE). Вид зв'язку залежить від самого пристрою, ніж воно більш сучасне, тим частіше він буде синхронізуватися з більш сучасним стандартом.

5G — майбутня основа телекомунікаційної мережі, а в ідеалі, рішення майбутніх проблем, які виникнуть на моделі 4G після того, як стандарт вступить широке застосування.

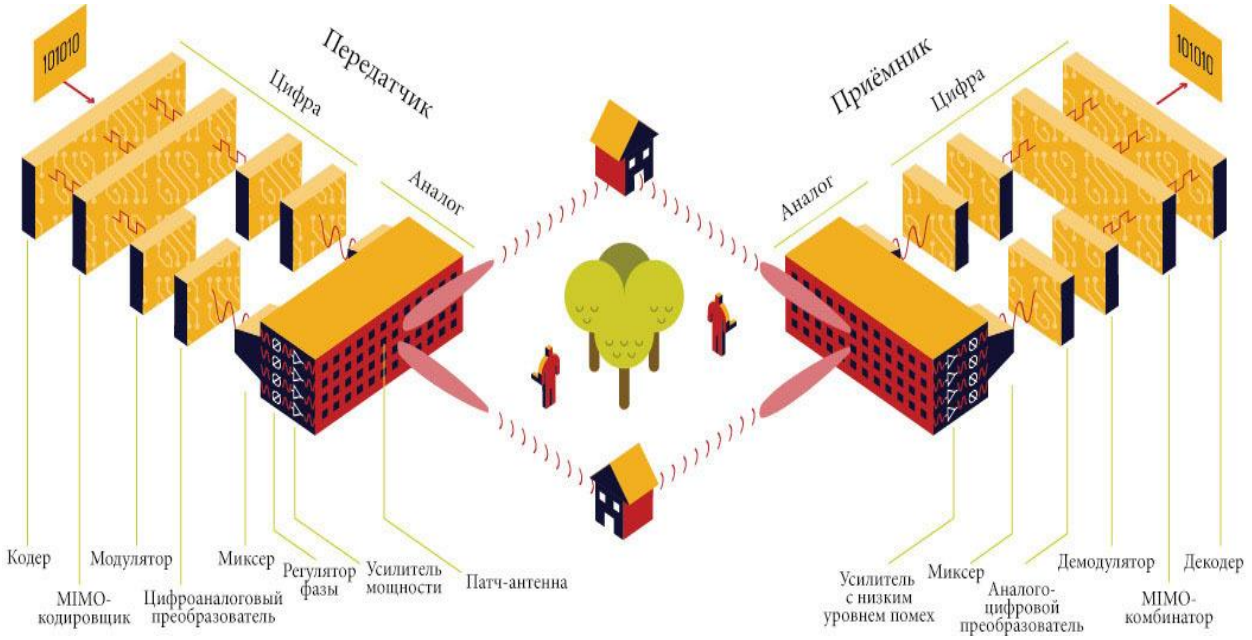
Мобільні мережі п'ятого покоління (5G) дозволять передавати інформацію зі швидкістю до 10 Гбіт/с та з часом відповіді на повідомлення будуть менше 1 мілісекунди, що задовольнить будь-які сучасні потреби із завантаження контенту. А також дасть поштовх к новим дослідам у сфері зв'язку,да і не тільки .

Першими результати своїх дослідів оголосила компанія Samsung, у середині 2013 р., в результаті проведених власних експериментів з прототипом електронної системи з обміну даних на частоті 28 ГГц між двома отримувачами, які рухалися зі швидкістю близько 8 км/год, досягнула щвидкості передачі 1.056 Гбіт/с , яка була у 10 разів вище ніж швидкість 4G.

Відстань при цьому становила приблизно 2 км прямої видимості . Прототип мережі від **Samsung** включає в себе масив з 64 антен розміром з таблетку, фазована антенна решітка, котра спрямовує сигнал в потрібну точку. Аналогові дані оцифровуються, що дозволяє тонко управляти сегментами масиву і **використовувати просторове мультиплексування** (MIMO). **Просторове мультиплексування** - це метод одночасної передачі незалежних потоків даних через різні антени для підвищення ефективної швидкості передачі. Оператор

може вибирати, чи відправляти дані на кілька пристрій одночасно або сконцентрувати промінь на одному пристрої, збільшивши швидкість скачування.

На малюнку будова 5G мережі від компанії Samsung .



Після цієї новини почали свої дослідження і інші великі компанії , всесвітні лідери з обладнання мереж мобільного зв'язку, такі як Nokia, Ericsson, Huawei. Nokia щодо здобуття першості у розвитку технології 5G та виведення її на ринок телекому, є об'єднання зусиль з потужною високотехнологічною компанією NationalInstruments задля створення експериментальної концептуальної системи 5G, реалізованої із застосуванням NI LabVIEW та модульних приладів NI PXI, які є на сьогодні найбільш сучасною системою для проведення експериментів і швидкого створення прототипів радіоінтерфейсу 5G .

Також важливо те, що **Компанії Nokia і Huawei сходяться в тому, що трафік в 5G буде коштувати не дорожче, ніж в 4G, інакше у споживачів не з'явиться бажання підключати пристрої до нових мереж. У будь-якому разі, поки рано говорити про те, на скільки 5G буде дорожче або дешевше діючих мереж зв'язку.**

Група дослідників британського Університету Суррея встановила рекорд швидкості для передачі даних по бездротових мережах.Займаючись розробкою стандарту зв'язку нового покоління 5G, **вчені зуміли досягти швидкості 1 Тбна відстані 100 метрів**.У 2016-2017 роках 5G InnovationCentre планує протестувати технологію на території університету, на великих відстанях.

Тоді південнокорейська компанія удосконалила технологію **Wi-Fi**, що дозволило передавати дані на швидкості **до 575 МБ / сек** у діапазоні 2 км.

Потім компанії **Alcatel-Lucent** і **BT** оголосили про досягнення рекордної швидкості передачі даних існуючої оптоволоконної мережі з використанням обладнання "комерційного класу". Експеримент проводився на лінії, прокладеної між радіотелевізійної передавальної станції BT Tower в центральному Лондоні і дослідницьким кампусом BT Adastral Park в Саффолку (графство Англії). **Відстань між передавачем і приймачем інформації склало приблизно 410 км , а швидкість составляла 1.4 Тб/с**!!.

Зараз ведеться активна дискусія по приводу **міліметрових хвиль .**
Міліметровий діапазон лежить в межах від 30 до 300 ГГц. Тривалий час ММВ вважалися непридатними для практичного використання , але пізніше почали впродовж досліджень ММВ почали показувати вражаючі результати .
І було відкрито , що ММВ мають дуже велику **пропускну здатність .**
У більшості випадків національний регулятивний орган може виділити ділянку шириною до 100 ГГц. Це більш ніж в 100 разів перевищує ширину діапазону, виділеного сьогодні на потреби стільникового зв'язку. Тобто, теоретично, оператори зможуть в 100 разів збільшити пропускну здатність у порівнянні з мережами LTE.

	Текущая технология	Миллиметровый диапазон
Длина одиночной антенны	На 700 МГц: 21,3 см	На 28 ГГц: 0,5 см
Максимальная дальность связи в городских условиях	На 700 МГц: 3 км	На 28 ГГц: 300 м
Затухание сигнала	На 700 МГц: Воздух: 0,005 дБ/км Ливень: 0,02 дБ/км	На 28 ГГц: Воздух: 0,1 дБ/км Ливень: 10 дБ/км

Також є новини з приводи появи 5G в Україні.

У Києві підписано меморандум про розвиток 5G в Україні
Компанії lifecell, Huawei і Ericsson підписала у вівторок меморандум про Сприяння розвитку п'ятого покоління мобільного зв'язку (5G) в Україні.

У підписання брали участь головний виконавчий директор lifecell Бурак Ерсой, директор компанії "Хуавей Україна" Чжоу Хаодзе і генеральний директор Ericsson в Україні Войцех Байда

Олександр Животовський, глава Національної комісії з питань регулювання зв'язку та інформатизації заявив що за офіційними даними та прогнозами 5G в Україні запустять у 2020 році , Україна стане однією з перших країн у світі, де впровадять 5G покриття.

Бут Олександр Дмитрович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ЩО ТАКЕ 5G МЕРЕЖА?
КОЛИ 5G З'ЯВИТЬСЯ В УКРАЇНІ?

Настало століття інновацій і високих технологій і у людини з'явилося багато додаткових можливостей. Гаджети з безліччю функцій, легкі комп'ютери і багато іншого. У всіх цих технологій є одна важлива функція, яка їх об'єднує - це доступ в Інтернет. Всі сучасні пристрої, які мають доступ в Інтернет, зараз використовують 3G і 4G (LTE). Вид зв'язку залежить від самого пристрою, ніж воно більш сучасне, тим частіше він буде синхронізуватися з більш сучасним стандартом.

5G — майбутня основа телекомунікаційної мережі, а в ідеалі, рішення майбутніх проблем, які виникнуть на моделі 4G після того, як стандарт вступить широке застосування.

Мобільні мережі п'ятого покоління (5G) дозволять передавати інформацію зі швидкістю до 10 Гбіт/с та часом відповіді на повідомлення будуть менше 1 мілісекунди, що задовольнить будь-які сучасні потреби із завантаження контенту.

Першими результати своїх дослідів оголосила компанія **Samsung**, у середині 2013 р., в результаті проведених власних експериментів з прототипом електронної системи з обміну даних на частоті 28 ГГц між двома отримувачами, які рухалися зі швидкістю близько 8 км/год, досягнула швидкості передачі 1.056 Гбіт/с. Відстань при цьому становила приблизно 2 км прямої видимості.Прототип мережі від **Samsung** включає в себе масив з 64 антен розміром з таблетку, фазована антенна решітка, котра спрямовує сигнал в

потрібну точку. Аналогові дані оцифровуються, що дозволяє тонко управляти сегментами масиву і **використовувати просторове мультиплексування** (MIMO). Оператор може вибирати, чи відправляти дані на кілька пристрій одночасно або сконцентрувати промінь на одному пристрої, збільшивши швидкість скачування.

Зараз ведеться активна дискусія по привіду **міліметрових хвиль .**
Міліметровий діапазон лежить в межах від 30 до 300 ГГц. І було відкрито , що ММВ мають дуже велику **пропускну здатність.** . Це більш ніж в 100 разів перевищує ширину діапазону, виділеного сьогодні на потреби стільникового зв'язку. Тобто, теоретично, оператори зможуть в 100 разів збільшити пропускну здатність у порівнянні з мережами LTE

Після цієї новини почали свої дослідження і інші великі компанії , всесвітні лідери з обладнання мереж мобільного зв'язку, такі як Nokia, Ericsson, Huawei.Nokia щодо здобуття першості у розвитку технології 5G та виведені її на ринок телекому, є об'єднання зусиль з потужною високотехнологічною компанією NationalInstruments задля створення експериментальної концептуальної системи 5G, реалізованої із застосуванням NI LabVIEW та модульних приладів NI PXI, які є на сьогодні найбільш сучасною системою для проведення експериментів і швидкого створення прототипів радіоінтерфейсу 5G .

Також важливо те, що **Компанії Nokia і Huawei сходяться в тому, що трафік в 5G буде коштувати не дорожче, ніж в 4G, інакше у споживачів не з'явиться бажання підключати пристрої до нових мереж. У будь-якому разі, поки рано говорити про те, на скільки 5G буде дорожче або дешевше діючих мереж зв'язку.**

Група дослідників британського Університету Суррея встановила рекорд швидкості для передачі даних по бездротових мережах.Займаючись розробкою стандарту зв'язку нового покоління 5G, **вчені зуміли досягти швидкості 1 Тб на відстані 100 метрів**. У 2016-2017 роках 5G InnovationCentre планує протестувати технологію на території університету, на великих відстанях в 2018 році

Тоді південнокорейська компанія удосконалила технологію **Wi-Fi**, що дозволило передавати дані на швидкості **до 575 МБ / сек.**

Що до появи 5G в Укріїні.

Компанії lifecell, Huawei і Ericsson підписали у вівторок меморандум про сприяння розвитку п'ятого покоління мобільного зв'язку (5G) в Україні.

У підписанні взяли участь головний виконавчий директор lifecell Бурак Ерсой, директор компанії "Хуавей Україна" Чжоу Хаодзе і генеральний директор Ericsson в Україні Войцех Байда.

Олександр Животовський, глава Національної комісії з питань регулювання зв'язку та інформатизації заявив що за офіційними данними та прогнозами 5G в Україні запустять у 2020 році , Україна стане однією з перших країн у світі, де впровадять 5G покриття.

Оприщенко Констяетин Антонович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ПОЯВА ХМАРНИХ СЕРВІСІВ СТАЛА МОЖЛИВОЮ У ПРОЦЕСІ РОЗВИТКУ ТЕХНОЛОГІЙ ХМАРНИХ ОБЧИСЛЕНЬ , ЯК ВІДОКРЕМЛЕНА ПОСЛУГА

Новітній Хмарні сервіси зазвичай здійснюються в мережі Інтернет за допомогою сучасних інтернет-браузерів. Для реалізації Хмарні сервіси використовують віртуальні машини, що функціонують у великих дата-центрах і замінюють собою фізичні персональні комп'ютери (ПК) та сервери. Головна відмінність від звичайного використання програмного забезпечення вХмарних сервісах полягає в тому, що користувач може поєднувати внутрішні ресурси свого комп'ютерного пристрою та програмні ресурси, які надаються йому як інтернет-сервіс. При цьому він має повний доступ до управління власними даними, але не може управляти операційною системою чи програмною базою, за допомогою яких ця робота відбувається.

Уперше ідею того, що кожна людина на Землі зможе отримувати з мережі не лише дані але й програми, висловив думку в 1970 р. американський вчений Джозеф Карл РобнеттЛіклайдер. Розширення пропускної здатності мережі Інтернет дало можливість компанії «Salesforce.com» у 1999 р. першою надати своє програмне забезпечення за принципом «програмне забезпечення як зовнішній сервіс». Значну роль у подальшому розвитку Хмарних сервісів відіграв розвиток технології віртуалізації. У 2006 р. компанія «Amazon» запустила перший вільно доступний сервіс під назвою ElasticComputecloud, який дозволяв його користувачам запускати свої власні додатки.

Більшість хмарних сховищпропонують майже необмежений функціонал безкоштовно, лімітуючи тільки обсяг даних. Додаткове місце можна купити за передплатою.

Необмежений функціонал Хмарних сервісів

У хмарних сервісах можна зберігати будь-які дані: від фотографій з пам'ятного пікніка, до особистих документів і робочих файлів. Причому, з робочими файлами можна працювати, ніби вони знаходяться у звичайній папці на вашому комп'ютері. Тобто, якщо ви на роботі працюєте з документом у хмарі і зберігаєте його, то вдома, чи на планшеті, чи в телефоні, ви зможете легко продовжити з ним працювати. Також, якщо ви збережетеся, зміни можна побачити на всіх пристроях, які підключені до вашого хмарного сервісу. Потрібен тільки Інтернет.

Сервіс дозволяє безкоштовно зберігати 2 ГБ даних.

100 ГБ будуть коштувати 10 доларів на місяць, є тарифи з 200 і 500 ГБ і «командні» тарифи від 1 ГБ. Окрім веб-інтерфейсу, є клієнти на всі мислимі і немислимі платформи. За їх використання на жорскому диску створюється тека, яка синхронізується із «хмарою». Є можливість посилатися на файли, які будуть доступними незареєстрованим користувачам. Деякі користувачі скаржаться на низьку швидкість завантаження. Але основною проблемою сервісу вважається необхідність самостійно шифрувати дані, тому що до безпеки сервісу є деякі питання.

Іноді, через схожу назву, з Dropbox плутають сервіс Box. Він розрахований більше на корпоративних користувачів, хоча пропонує широку функціональність і для звичайних людей. Безкоштовно пропонується 5 ГБ (з обмеженням розміру одного файлу в 250 Мб). За $ 11.5 в місяць можна отримати відразу 25 ГБ. Професійні тарифи починаються з 13 доларів в місяць на одиницю користувача (їх повинно бути мінімум три), а розмір для трійці пропонується вже від терабайта.
МінусомBoxможнаназватиобмеженняфункціональності для безкоштовнихкористувачів. В тому числішвидкостізавантаження, а такожінтеграції з сервісамиGoogle, повнотекстовогопошуку та історіїверсій файлу.Безкоштовнимкористувачамнедоступнийофіційнийклієнт для Windows (хоча є і сторонні), відсутніклієнти для деякихзастарілихаборідкісних ОС. Професійнітарифидорогі, але сервісBox – вважаєтьсядоситьнадійним і безпечнимсервісуправлінняпроцесами (Process-as-a-Service) є віддаленим ресурсом, якийможезв'язативоєдинокількаресурсів, таких як послугиабодані, щомістяться в межах однієї хмари абоіншихдоступниххмарах, для створенняєдиногобізнес-процесу.Бізнес-процесможна подати як додаток, щоінтегруєбазовіпослуги та інформацію, якіскомбіновані в певнупослідовність, щоформуєпроцес. Такіпроцесизавждилегшезмінювати, ніжсамідодатки; додаток як сервіс (Application-as-a-Service) можематиназву «програмнезабезпечення як сервіс» (Softwareas a Service), тобто будь-

якийдодатокабопрограма, якікористувачможезапускати через інтернет; сервіс-платформа (Platform-as-a-Service) — цеповна платформа, щомістить додатки, інтерфейси, базиданих, їхзберігання і тестування; сервіс.

Литература:
1.Онлайновые хранилища данных // ComputerBild : журнал. — 2010. — № 4. — С. 62—67.
2.Масштабные утечки данных: конец «облачным» сервисам? // Chip : журнал. — 2011. — № 8 (149). — С. 20—21. — ISSN 1609-4212

Оприщенко Констяетин Антонович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ХМАРНІ СХОВИЩА

Де надійно зберегти своє все.

Новітній вид мережевих послуг, які дозволяють інформаційними засобами віртуального середовища розширити програмно-технічні ресурси комп'ютерного пристрою користувача.

ПоявиХмарних сервісів стала можливою у процесірозвиткутехнологійхмарнихобчислень , як відокремленапослуга.

Новітній Хмарні сервіси зазвичай здійснюються в мережі Інтернет за допомогою сучасних інтернет-браузерів. Для реалізації Хмарні сервіси використовують віртуальні машини, що функціонують у великих дата-центрах і замінюють собою фізичні персональні комп'ютери (ПК) та сервери. Головна відмінність від звичайного використання програмного забезпечення вХмарних сервісах полягає в тому, що користувач може поєднувати внутрішні ресурси свого комп'ютерного пристрою та програмні ресурси, які надаються йому як інтернет-сервіс. При цьому він має повний доступ до управління власними даними, але не може управляти операційною системою чи програмною базою, за допомогою яких ця робота відбувається.

Уперше ідею того, що кожна людина на Землі зможе отримувати з мережі не лише дані але й програми, висловив думку в 1970 р. американський вчений Джозеф Карл РобнеттЛіклайдер. Розширення пропускної здатності мережі Інтернет дало можливість компанії «Salesforce.com» у 1999 р. першою надати своє програмне забезпечення за принципом «програмне забезпечення як зовнішній сервіс». Значну роль у подальшому розвитку Хмарних сервісів відіграв розвиток технології віртуалізації. У 2006 р. компанія «Amazon»

запустила перший вільно доступний сервіс під назвою ElasticComputecloud, який дозволяв його користувачам запускати свої власні додатки.

Більшість хмарних сховищпропонують майже необмежений функціонал безкоштовно, лімітуючи тільки обсяг даних. Додаткове місце можна купити за передплатою.

НеобмеженийфункціоналХмарнихсервісів

У хмарних сервісах можна зберігати будь-які дані: від фотографій з пам'ятного пікніка, до особистих документів і робочих файлів. Причому, з робочими файлами можна працювати, ніби вони знаходяться у звичайній папці на вашому комп'ютері. Тобто, якщо ви на роботі працюєте з документом у хмарі і зберігаєте його, то вдома, чи на планшеті, чи в телефоні, ви зможете легко продовжити з ним працювати. Також, якщо ви збережетеся, зміни можна побачити на всіх пристроях, які підключені до вашого хмарного сервісу. Потрібен тільки Інтернет.

Хмарні.сервіси за формою подання можуть бути розділені на такі категорії: додатки, платформи та інфраструктури, серед яких виділяють більш деталізовані типи: 1) як сервіс зберігання даних (Storage-as-a-Service), дисковий простір на вимогу. Ця послуга дає можливість зберігати дані в зовнішньому сховищі у «хмарі». Для користувача це додатковий логічний диск або папка. Сервіс є базовим для інших Х.с., оскільки входить до складу практично кожного з них; 2) сервіс баз даних (Database-as-a-Service), який надає

можливості працювати з базами даних так, ніби система управління базами даних була встановлена на локальному ресурсі. У цьому разі набагато легше організовувати передачу інформації між різними виконавцями та додатками; 3) інформаційний сервіс (Information-as-a-Service), дає можливість віддалено використовувати будь-які види та архіви інформації (інсайдерська та галузева інформація для технічного і фундаментального аналізу, новинні стрічки телеграфних агентств,

Сервіс дозволяє безкоштовно зберігати 2 ГБ даних.

100 ГБ будуть коштувати 10 доларів на місяць, є тарифи з 200 і 500 ГБ і «командні» тарифи від 1 ГБ. Окрім веб-інтерфейсу, є клієнти на всі мислимі і немислимі платформи. За їх використання на жорскому диску створюється тека, яка синхронізується із «хмарою». Є можливість посилатися на файли, які будуть доступними незареєстрованим користувачам. Деякі користувачі скаржаться на низьку швидкість завантаження. Але основною проблемою сервісу вважається необхідність самостійно шифрувати дані, тому що до безпеки сервісу є деякі питання.

Іноді, через схожу назву, з Dropbox плутають сервіс Box. Він розрахований більше на корпоративних користувачів, хоча пропонує широку функціональність і для звичайних людей. Безкоштовно пропонується 5 ГБ (з обмеженням розміру одного файлу в 250 Мб). За $ 11.5 в місяць можна отримати відразу 25 ГБ. Професійні тарифи починаються з 13 доларів в місяць на одиницю користувача (їх повинно бути мінімум три), а розмір для трійці пропонується вже від терабайта.

Мінусом Box можна назвати обмеження функціональності для безкоштовних користувачів. В тому числі швидкості завантаження, а також інтеграції з сервісами Google, повнотекстового пошуку та історії версій файлу. Безкоштовним користувачам недоступний офіційний клієнт для Windows (хоча є і сторонні), відсутні клієнти для деяких застарілих або рідкісних ОС. Професійні тарифи дорогі, але сервіс Box – вважається досить надійним і безпечнимсервіс управління процесами (Process-as-a-Service) є віддаленим ресурсом, який може зв’язати воєдино кілька ресурсів, таких як послуги або дані, що містяться в межах однієї хмари або інших доступних хмарах, для створення єдиного бізнес-процесу. Бізнес-процес можна подати як додаток, що інтегрує базові послуги та інформацію, які скомбіновані в певну послідовність, що формує процес. Такі процеси завжди легше змінювати, ніж самі додатки; додаток як сервіс (Application-as-a-Service) може мати назву «програмне забезпечення як сервіс» (Softwareas a Service), тобто будь-який додаток або програма, які користувач може запускати через інтернет; сервіс-платформа (Platform-as-a-Service) — це повна платформа, що містить додатки, інтерфейси, бази даних, їх зберігання і тестування; сервіс-інтеграція програм (Integration-as-

a-Service) — можливість отримувати з хмари повний інтеграційний пакет, у тому числі програмні інтерфейси між додатками, семантичну медіацію, управління алгоритмом і дизайн інтегрованого пакета. Сюди входять відомі послуги і функції пакетів централізації, оптимізації та інтеграції корпоративних додатків; сервіс-безпека (Security-as-a-Service) — забезпечує безпечний доступ до корпоративної інформації, у тому числі ідентифікацію користувача, розпізнавання прав доступу тощо, які надаються з хмари; сервіс адміністрування та управління (Management/Governace-as-a-Ser-vice) дає можливість керувати і задавати параметри роботи одного або багатьох Х.с.: топологія, використання ресурсів, віртуалізація, тимчасові параметри роботи сервісів; сервіс інфраструктур (Infrastructureas a Service) надає клієнту комп'ютерні інфраструктури: сервери, системи зберігання даних, мережеве устаткування, а також програми для управління цими ресурсами (замовник сплачує лише за те, що йому в певний час необхідно, з можливістю гнучкого збільшення чи зменшення обсягу використаних ресурсів); сервіс-дані (Desktopas a Service) клієнти отримують повністю готове до роботи стандартизоване віртуальне робоче місце, яке кожен користувач може додатково налаштовувати під свої завдання. Користувач отримує доступ не до окремої програми, а до програмного комплексу, необхідного для повноцінної роботи; сервіс робоче місце (Workspaceas a Service) — на відміну від попереднього сервісу дозволяє користувачеві отримувати доступ лише до програмного забезпечення, а всі обчислення відбуваються безпосередньо на ПК користувача.

Публічні хмари та їх використання

За способом використання Хмарні сервіси поділяють на: публічні хмари, що використовуються безліччю компаній та сервісів. Користувачі в публічній хмарі не мають можливості управляти й обслуговувати ці хмари, вся відповідальність з цих питань покладена на власника хмари. Абонентом такого сервісу може стати будь-яка компанія чи індивідуальний користувач; приватні хмари, що контролюються та експлуатуються в інтересах єдиної організації. Організація може керувати приватною хмарою самостійно чи доручити це завдання зовнішньому підряднику; гібридні хмари, що використовують особливості публічної та приватної хмари при вирішенні поставленого завдання. Такий тип хмар часто використовують, якщо організація має сезонні періоди активності; якщо внутрішня інфраструктура не справляється з поточними завданнями, частина потужностей перекидається на публічну хмару, а також для надання доступу користувачам до ресурсів підприємства (до приватної хмари) через публічну хмару.

Хмарні сервіси в освіті розглядаються як найбільш перспективний розвиток упровадження хмарних технологій. На сьогодні найбільшими постачальниками програмного контенту для навчальних закладів є компанії «Microsoft» і

«Google», що надають програмні та інфраструктурні сервіси школам, коледжам і університетам. Прикладами сучасних сервісів, побудованих на основі хмарних обчислень для освіти, є Live @ edu від Microsoft і GoogleAppsEducationEdition. Основні недоліки Хмарних сервісів — необхідність забезпечення постійного з'єднання з мережею Інтернет та відсутність технологій гарантування збереження та конфіденційності даних.

Литература:
1.Онлайновые хранилища данных // ComputerBild : журнал. — 2010. — № 4. — С. 62—67.
2.Масштабные утечки данных: конец «облачным» сервисам? // Chip : журнал. — 2011. — № 8 (149). — С. 20—21. — ISSN 1609-4212

Акинтола Муїва Олувасеун
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

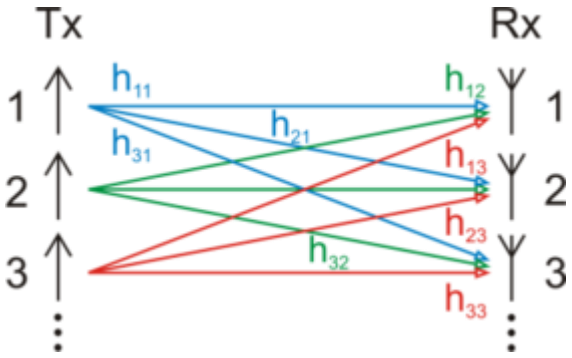
ТЕХНОЛОГИЯ MIMO

MIMO (англ. *Multiple Input Multiple Output*) — метод пространственного кодирования сигнала, позволяющий увеличить полосу пропускания канала, в котором передача данных и прием данных осуществляются системами из нескольких антенн. Передающие и приёмные антенны разносят так, чтобы корреляция между соседними антеннами была слабой.

В современных системах связи, например, в сотовых системах связи, высокоскоростных локальных вычислительных сетях и др., существует необходимость повышения пропускной способности. Пропускная способность может быть увеличена путём расширения полосы частот или повышения излучаемой мощности. Тем не менее, применимость этих методов ограничена из-за требований биологической защиты, ограниченной мощности источника питания (в мобильных устройствах) и электромагнитной совместимости. Поэтому если в системах связи эти подходы не обеспечивают необходимую скорость передачи данных, то эффективным может оказаться применение адаптивных антенных решёток со слабо коррелированными антенными элементами. Системы связи с такими антеннами получили название систем MIMO.

В общем случае в канале наблюдаются межсимвольная интерференция и частотная селективность, но во многих случаях длительность импульсов в беспроводных системах связи намного больше задержек сигналов,

поступающих на приёмную антенну, что даёт возможность пренебрегать межсимвольной интерференцией в канале. Частотную селективность также приходится принимать во внимание, например, в системах связи стандарта IEEE 802.11, где используется технология OFDM. Однако в некоторых ситуациях можно использовать модель канала без частотной селективности.



Обработка сигналов на приёмной стороне MIMO-системы

Среди алгоритмов обработки сигналов на приёмной стороне можно выделить:

- алгоритмы, основанные на методе максимального правдоподобия (maximum likelihood, ML);
- алгоритмы, основанные на методе минимальных среднеквадратичных отклонений (МСКО);
- алгоритмы, основанные на методе форсирования нуля (обнуления, англ. *zero forcing*, ZF).

Также существует разделение на ортогональные и неортогональные методы кодирования/декодирования.

Основной задачей любого метода является поиск решений из числа всех возможных по наименьшему евклидовому расстоянию между переданным символом и одним из возможных решений.

Литература

- *Бакулин М. Г., Варукина Л. А., Крейнделин В. Б.* Технология MIMO: принципы и алгоритмы. — М.: Горячая линия - Телеком, 2014. — 242 с. — ISBN 978-5-9912-0457-6.
- *Сперанский В. С., Евдокимов И. Л.* Моделирование сигналов OFDM-MIMO систем беспроводной передачи данных 802.16, Труды Московского технического университета связи и информатики. — М:МТУСИ, 2007.
- *Бакулин М. Г., Крейнделин В. Б., Шлома А. М.* Новые технологии в системах мобильной радиосвязи. — М:Инсвязьиздат, 2005.
- Флаксман А. Г. Адаптивная пространственная обработка в многоканальных информационных системах// Дис. Д-ра физ.-мат. наук . — М.: РГБ 2005 (Из фондов Российской Государственной библиотеки)

Наукове видання

«СВІТ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЇ »

Збірник матеріалів
ІІІ Міжнародної науково-технічної конференції студентства та молоді

Київ, 26 грудня 2016 року

Редагування: Бондаренко Є., Приходько В., Кравченко Р.,
Школьний І.А., Щетініна А.А.
Відповідальні за випуск: Бондаренко Є., Приходько В., Кравченко Р.,
Школьний І.А., Щетініна А.А.

Подано до друку 25.12.16
Формат 60х84. Папір друкарський. Гарнітура «Time New Roman».

Державний університет телекомунікацій
вул. Солом'янська, 7, м. Київ, 03110, Україна

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Контакти

dut.edu.ua

vk.com/stydrada_dut