МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ТЕЛЕКОМУНІКАЦІЙ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ

Матеріали Всеукраїнської науково-практичної конференції

23 лютого 2023 року

КИЇВ

УДК: 004.056

Рекомендовано до друку Вченою радою Навчально-наукового інституту захисту інформації Державного університету телекомунікацій

(протокол № 6 від 17.02.2023 р.)

Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:

Матеріали Всеукраїнської науково-практичної Інтернет-конференції (м. Київ, 23 лютого 2023 року) / Навчально-науковий інститут захисту інформації ДУТ. Київ, 2023. 149 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з інформаційної та кібернетичної безпеки, працівників органів державної влади та місцевого самоврядування.

Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Тези подані в авторській редакції та відображають персональну позицію учасників конференції

ЗМІСТ

СЕКЦІЯ 1. СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

ОЦІНКА ЕФЕКТИВНОСТІ ПРОЦЕСУ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Рой І. В.
Державний університет телекомунікацій
м. Київ, Україна

Інциденти інформаційної безпеки є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інфо-соціо-технічній інфраструктурі держави, і, як окремий випадок, – в організаційно-технічних системах та інформаційно-комунікаційних мережах, впливаючи на стан державних інформаційних ресурсів і національної безпеки [1, с. 116].

Розвиток інформаційних технологій призводить до збільшення випадків витоку інформації. Одним із важливих засобів захисту інформації є система управління інцидентами інформаційної безпеки.

Незалежно від кількості вже проваджених засобів захисту в організації, якщо своєчасно не реагувати на виникаючі загрози інформаційної безпеки, то їх ефективність буде прагнути до нуля. При цьому з ростом обсягів інформаційних потоків стрімко зростає і кількість засобів ІБ, від яких надходять дані про події інформаційної безпеки, тому встежити за рівнем безпеки організації стає все складніше і складніше [4, с. 104].

В контексті забезпечення інформаційної безпеки визначальним є комплексний підхід щодо виявлення інцидентів інформаційної безпеки, реагування на них, а також проведення аналізу інцидентів для того, щоб спланувати превентивні заходи захисту та вдосконалити процес забезпечення інформаційної безпеки в цілому. Процес управління інцидентами виступає визначальним джерелом даних для аналізу системами менеджменту інформаційної безпеки, проведення оцінки ефективності заходів щодо зниження ризиків та планування покращень в роботі системи

На сьогодні в міжнародній практиці представлено значний спектр нормативних документів, які регламентують питання управління інцидентами інформаційної безпеки. Аспект управління інцидентами є актуальним як в контексті забезпечення інформаційної безпеки, так і в сфері управління IT-сервісами в цілому. Зокрема, в рамках стандарту ISO / IEC 27001:2018 «Information technology – Security techniques – Information security management systems – Overview and vocabulary» представлені загальні вимоги до побудови системи управління інформаційною безпекою, які в тому числі відносяться і до процесів управління інцидентами [2, с. 48].

В документі CMU / SEI – 2004-TR – 015 «Defining incident management processes for CISRT» представлено методологію планування, впровадження, оцінки та покращення процесів управління інцидентами. Значна увага

приділяється задачам організації роботи CISRT (Critical Incident Stress Response Team) – команди або структурного підрозділу, що здійснює забезпечення попередження, обробки та реагування на інциденти інформаційної безпеки, а також наводиться спектр критеріїв, що дають змогу оцінити ефективність даних сервісів. В NIST SP 800–61 «Computer security incident handling guide» представлено збірку «найкращих практик» побудови процесів управління інцидентами та реагування на них.

Для обробки інцидентів інформаційної безпеки необхідно організувати процес реагування на інциденти, що враховує аналіз загроз та пошук вразливостей, проведення аналізу та аудиту журналів подій, що обумовлені функціонуванням інформаційної інфраструктури, відповідного реагування на основі отриманого досвіду на інциденти та розробку заходів, які сприяють вдосконаленню діючих процесів в контексті інформаційної безпеки. Управління інцидентами інформаційної безпеки здійснюється в рамках діючих вимог стандартів інформаційної безпеки [3, с. 165].

Отже, ефективна система управління інцидентами інформаційної безпеки дозволить зменшити негативний вплив інцидентів на діяльність організації, покращить захищеність критичних інформаційних ресурсів та інфраструктури, а також сприятиме превентивному визначенню заходів щодо покращення інформаційної захищеності.

Література

1. Гладиш С. В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. *Реєстрація, зберігання і обробка даних.* 2008 Т. 10, № 1. С. 116–124.
2. Корченко О. Г., Гнатюк С. О. Казмірчук С. В. Аудит та управління інцидентами інформаційної безпеки. СБ України, 2014. 190 с.
3. Панаско О. М., Бурмістров С. В. Практичні аспекти управління інцидентами інформаційної безпеки. *International scientific journal «Grail of Science».* № 5. 2021. С. 164–166.
4. Ушатов В., Сєвєрінов О. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. *Global Cyber Security Forum*: матер. Першого між нар. наук. – практ. форуму. 2019 р. Харків: ХНУРЕ, 2019. С. 104–105.

СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА ПОДІЯМИ (SIEM), ЯК ОДИН ІЗ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

Карачун Б.О.
Державний університет телекомунікацій
м. Київ, Україна

Актуальність: Інформація про безпеку та управління подіями (SIEM) в умовах сучасності стали вагомою складовою забезпечення безперервності та безпеки бізнесу [1]. В умовах загострення конкуренції й при численних фактах інформаційних витоків бізнес- процеси залишаються вразливими до несанкціонованих втручань. У будь-якій галузі будь-якого масштабу бізнес може зіштовхнутися із всілякими подіями інформаційної безпеки, які можуть привести до негативних наслідків державної або комерційної організації (компанії, підприємства) у напрямку порушення безперервної діяльності і взагалі - припинення виконання функціональних задач. І чим більше використовуються в бізнесі інформаційні технології, тем серйозніше він потребує забезпечення безперервності процесів й відновлення після їх збоїв. Хоч система (SIEM) самостійно нічого не попереджає і не захищає, проте вона аналізує інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів і призначених для користувача ПК, і при цьому детектує відхилення від норм по певним критеріям. Відповідно, система забезпечує автоматизацію моніторингу та аналізу всіх подій, які відбуваються в численних системах захисту компанії, створюючи умови для проактивного реагування на події в компанії.

По мірі того, як бізнеси оновлюють і покращують масштабність все більш складних IT-інфраструктур, SIEM набуває ще більшого. Всупереч поширеній думці, брандмауерів та антивірусних пакетів недостатньо для захисту мережі в цілому. Відповідно дослідження сучасних SIEM систем для забезпечення безперервності бізнесу залишається актуальним.

Проблема дослідження. SIEM системи не тільки забезпечують управління інцидентами, а також контролюють помилки і збої в операційних системах, мережевому обладнанні, програмному забезпеченні. Це дозволяє бізнесам працювати безупинно та нарощувати потужності, адже будь який збій у інформаційній системі перериває ті чи інші бізнесові процеси, негативно впливаючи на виробництво та завдаючи репутаційних ударів. Проте, донині спостерігається ряд проблем з функціонуванням системи управління інформацією та подіями (SIEM): некваліфіковане розслідування інцидентів, аудиту і тестів на проникнення, незадовільне налаштування і обслуговування для адекватного реагування на зміни середовища, погроз, вимог регуляторів або даних тощо. Названі та інші проблеми, оскільки вони негативно впливають на процес безперервності бізнесу, будуть досліджені у роботі.

Метою роботи є дослідження аспектів функціонування системи управління інформацією та подіями задля забезпечення безперервності бізнесу.

Об'єкт дослідження – ризики у системах управління інформацією та подіями (SIEM).

Метод дослідження – аналітичний з використанням сучасної бази міжнародних наукових досліджень за темою.

SIEM (Security information and event management) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Поняття управління подіями інформаційної безпеки (SIEM), введене Марком Ніколетта і Амріта Вільямсом з компанії Gartner в 2005 р[2].

Зі зростаючим обсягом інформації, яка обробляється і передається між різними інформаційними системами, бізнеси все більше залежать від безперервності і коректності виконання даних процесів.

Випереджаюче управління інцидентами і подіями безпеки полягає в прийнятті рішень ще до того, як ситуація стане критичною [3]. Таке управління може здійснюватися з використанням автоматичних механізмів, які прогнозують майбутні події на основі історичних даних, а також автоматичного підстроювання параметрів моніторингу подій до конкретного стану системи. Такі можливості SIEM систем створюють подушку безпеки для бізнесу, адже дають можливість прорахувати і попередити майбутні ризики.

Відповідно до стандарту ISO/IEC 27032:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо кібербезпеки», на системи управління інформацією та подіями покладаються завдання щодо забезпечення умов, спрямованих на досягнення і збереження властивостей безпеки у ресурсах бізнесу[4].

Поскільки SIEM - це складна комплексна система, що дозволяє отримувати своєчасну і повну інформацію про стан IT-інфраструктури бізнесу, керівникам варто надавати значної уваги щодо функціонування цих систем на практиці. Підготовка фахівців, здатних аналізувати дані систем потребує від бізнесі додаткових капіталовкладень, адже складний процес впровадження і вимога до безперервного забезпечення збору подій і управління правилами кореляції вимагає наявність в штаті компанії кваліфікованих співробітників або залучення фахівців зі сторони інтегратора. Установка SIEM-системи без належного контролю і управління буде лише додатковою витратою бюджету.

З іншого боку самі системи SIEM потребують постійного оновлення та прогресивного розвитку, особливо щодо розширення та чіткої класифікації «подій безпеки». Також особливої уваги потребує процес моделювання і формуваня нових правил виявлення інформаційних загроз і оцінки рівня їх критичності, в залежності від нових викликів та кіберзагроз.

Проведений аналіз показав, SIEM дозволяє акцентувати увагу тільки на критичних і дійсно важливих загрозах, працювати не з подіями, а з інцидентами, своєчасно виявляти аномалії і ризики, запобігати фінансовим втратам і підвищувати ефективність і безпеку роботи бізнесу в цілому. Проте, є й важливі завдання модифікації названих систем. Проблемним питанням залишається

детальне планування перед покупкою SIEM системи. Без попереднього планування ймовірність успішної реалізації SIEM-проекту майже нульова, а витрати часу, ресурсів і фінансів будуть набагато переважувати передбачувані вигоди. Тому через складність і високі вимоги системи безпеки SIEM часто не виправдовують очікування керівництва і користувачів, мета їх використання не досягається. Крім того, однією з найпоширеніші причини невдалих SIEM-проектів є брак кваліфікованих ресурсів і навичок обслуговуючого персоналу (фахівців з досвідом з розслідування інцидентів, аудиту і тестів на проникнення). SIEM система потребує постійної настройки і обслуговування для адекватного реагування на зміни середовища, погроз, вимог регуляторів або даних. Існує також низька проблем, пов‘язаних з технічними питаннями застосування систем управління інформаційною безпекою та подіями безпеки.

Але, незважаючи на достатню кількість проблемних питань при використанні SIEM-систем, вони остаються ефективним засобом протидії інцидентам інформаційної безпеки. Тому необхідно продовжувати роботу щодо їх модернізації, покращенню їх параметрів та можливостей.

Література

1. Столова О. В. Методика порівняння ефективності сучасних SIEM-систем: URL:http://ela.kpi.ua/bitstream/123456 789/20810/1/13.%D0%A1%D1%82%D0%BE%D0%BB%D0%BE%D0%B2%D0% B0.163- 164.pdf
2. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. Харків: ХНУРЕ, 2019.
3. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення, Київ: НАУ, 2011.
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від від 26.08.2021р. № 447.URL: https://zakon.rada.gov.ua/go/n0055525-21

СЕКЦІЯ 2. НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА ЗБРОЙНИХ СИЛ УКРАЇНИ

Грибенко Р.В.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Зміст інформаційної та кібербезпеки Збройних Сил України визначається офіційно прийнятими поглядами на шляхи забезпечення оборони при запобіганні виникненню воєнних конфліктів, стримуванні потенційного агресора в разі виникнення передумов застосування воєнної сили та відсічі збройній агресії [1].

Існуючі воєнно-політичні виклики переросли в цілеспрямований інформаційний (інформаційно-психологічний) вплив і стали загрозою для дестабілізації соціально-політичної обстановки в Україні та мають тенденції до постійно погіршення.

Зазначена ситуація вказує на недостатню інформаційну протидію як збоку держави, так і Збройних Сил України в цілому. Тому інформаційна та кібербезпека Збройних Сил України, повинна бути спрямована на попередження загроз застосування воєнної сили проти України, та формування позитивного міжнародного іміджу України, а також на стабілізацію внутрішніх загострень міжетнічних та міжконфесійних відносин в Україні [2].

Організація та проведення відповідних інформаційних заходів здійснюється всіма суб'єктами забезпечення оборони України відповідно до їхньої компетенції.

Що стосується Генерального штабу Збройних Сил України, то розподіл функцій щодо реалізації інформаційної та кібербезпеки, організації та проведення інформаційних заходів в інтересах оборони держави, між ними визначається відповідними Положеннями, затвердженими Указом Президента України [1].

Так, Міністерство оборони України відповідно до покладених на нього завдань:

- проводить постійний моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози в оборонній сфері, здійснює попереджувальні інформаційні заходи;
- забезпечує впровадження та розвиток новітніх інформаційних технологій у сфері оборони.

Крім того, Міністерство оборони України виконує загальну функцію планування та здійснення заходів щодо протидії і нейтралізації воєнно-політичних ризиків, викликів, загроз застосування воєнної сили проти України,

до яких відносяться (згідно Воєнної Доктрини України) такі, які вимагають обов'язкового проведення комплексу інформаційних заходів, спрямованих на їх нейтралізацію:

- втручання у внутрішні справи України з боку Російської Федерації, спрямоване на порушення конституційного устрою, територіальної цілісності та суверенітету України, внутрішньої соціально-політичної стабільності та правопорядку;
- протидія реалізації європейського вибору Українського народу, формуванню систем колективної безпеки за участю України;
- невирішеність питань щодо розмежування державного кордону України в акваторії Чорного і Азовського морів, незавершеність договірно-правового оформлення державного кордону України з Російською Федерацією, Республікою Білорусь та Республікою Молдова;
- інформаційні операції з боку Російської Федерації спрямовані на погіршення соціально-політичної та економічної ситуації в Україні, а також провокування сепаратистських настроїв у районах компактного проживання національних меншин на території України;
- цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, з боку Російської Федерації;
- дії Російської Федерації щодо ускладнення та уповільнення економічного розвитку України;
- розповсюдження зброї масового ураження, тероризму, організована злочинність, незаконна торгівля зброєю і боєприпасами, нелегальна міграція.

В свою чергу, Генеральний штаб Збройних Сил України відповідно до покладених на нього завдань:

- забезпечує інформаційну безпеку у Збройних Силах України;
- у питаннях виконання завдань особливого періоду бере участь в організації використання повітряного, водного, інформаційного простору держави та здійснює контроль за їх використанням.

Таким чином, саме Міністерство оборони України відповідає за реалізацію інформаційної та кібербезпеки, проведення інформаційних заходів реагування на потенційні та реальні інформаційні загрози в оборонній сфері. Однак, на практиці, існує проблема залучення до проведення цих заходів військових частин Збройних Сил України, яка має як об'єктивне, так і суб'єктивне підґрунтя.

Література

1. Закон Про оборону України: за станом на 01.07.2018 р./, затверджений ВР України від 06.12.1991, № 1932-XII. URL: http://zakon4.rada.gov.ua/laws/show/1932-12.
2. Закон України Про Збройні Сили України від 6 грудня 1991 року N 1934-XII (зі змінами). URL: http://zakon3.rada.gov.ua/laws/show/1934-12.

ОСОБЛИВОСТІ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ В УМОВАХ ШИРОКОМАСШТАБНОЇ ВІЙНИ

Іванів В.І.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Дії російсько-терористичних військ у зоні проведення операції об'єднаних сил суттєво підвищують вимоги до розвідки. Важливим напрямком розвідувальної діяльності в інтересах органів військового управління й надалі залишається постійний та цілеспрямований моніторинг відкритих джерел інформації, у тому числі й інформаційних ресурсів мережі інтернет на предмет виявлення в їх контенті ознак інформаційних операцій проти України. Одержувані у результаті такого моніторингу оцінки рівня загроз інформаційній безпеці держави у воєнній сфері суттєво доповнюють загальну оцінку рівня загрози національній безпеці України [1, с. 21].

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Проти України застосовуються різноманітні інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Боротьба за перевагу у світовому інформаційному просторі провокує різке зростання реальних та потенційних загроз інформаційній безпеці України. Для ефективного формування системи захисту та протидії негативному інформаційному впливу існує необхідність розглядати загрози національній безпеці нашої держави в інформаційній сфері комплексно за всіма сферами. Загрози проявляються у зовнішньополітичній та внутрішньополітичній сферах, у сфері державної безпеки, науково-технологічній, економічній, соціальній та гуманітарній сферах [2, с. 30].

Водночас за сучасних умов найбільшу небезпеку становлять загрози у воєнній сфері, і саме проблема інформаційної безпеки воєнній організації держави у контексті жорсткого інформаційного протистояння під час проведення антитерористичної операції викликає найбільшого занепокоєння і потребує найбільшого зосередження органів державної влади та спеціальних служб [3, с. 18].

В умовах гібридної агресії Росії проти України державна інформаційна політика передусім зосереджується на реалізації системи заходів щодо протидії руйнівному інформаційному впливу Кремля, насамперед:

- запобігання інформаційним загрозам (викликам, впливам) шляхом здійснення превентивних заходів із забезпечення інформаційної безпеки держави;

- виявлення інформаційних загроз та деструктивних впливів, яке полягає у систематичному моніторингу, аналізі й прогнозуванні появи реальних або потенційних інформаційних загроз;
- ліквідацію наслідків негативних інформаційних впливів.

Важливим етапом при реалізації заходів пов'язаних з виявленням деструктивних впливів, є процедура моніторингу та оцінювання загроз інформаційній безпеці України в цілому та у воєнній сфері зокрема. При цьому у воєнній сфері така процедура має свої та властиві лише їй специфічні особливості, які передбачають:

- по-перше, виявлення негативного зовнішнього впливу на особовий склад Збройних Сил нашої держави, його аналіз за якісними і кількісними показниками, визначення форм та способів інформаційної боротьби;
- по-друге, встановлення та доведення факту наявності в ньому інформаційних загроз державі у воєнній сфері та оцінювання рівня цих загроз.

Однією з причин актуалізації проявів інформаційних загроз державі є швидкі темпи розвитку та впровадження у повсякденне життя інформаційних технологій, що тісно пов'язані з розвитком мережі Інтернет. Завдяки ній користувачі, у тому числі й військовослужбовці ЗС України, задовольняють власні інформаційні потреби, обумовлені не тільки приватною, а й професійною діяльністю.

Наявні факти наочно доводять ефективність інформаційної зброї на сучасному етапі розвитку військового мистецтва. Інформаційні загрози сьогодні стали настільки ефективними засобами маніпулювання суспільством, що здатні зумовлювати появу, перебіг і кінцевий результат не лише політичних подій в державі, а навіть глобальних проблем миру й війни.

Основна небезпека від проявів інформаційних загроз у воєнній сфері полягає в тому, що на перший план все більше висуваються технології інформаційно-психологічного впливу, які дозволяють перетворити державу-опонента в регіон керованої кризи. Такі технології представлені різноманітними засобами маніпулювання індивідуальною та суспільною свідомістю. Зокрема вони призводять до етнічного сепаратизму і внутрішньої регіоналізації, нав'язування чужої мови і культури тощо. У поєднанні з політико-дипломатичним тиском, що спирається на економічну та військову силу, такі технології стають більш ефективними, ніж застосування сучасних засобів збройної боротьби.

Отже, досвід сучасної агресії РФ показав, що сьогодні перед органами військового управління, відповідальними за інформаційну безпеку держави у воєнній сфері, стоїть ряд важливих та складних завдань, одним з яких є визначення джерел воєнної небезпеки, встановлення характеру та ступеня воєнних загроз державі, а також факторів, що можуть вплинути на хід та результати збройного конфлікту.

Література
1. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 469 с.
2. Дубов Д. Стан та проблеми забезпечення державної інформаційної політики: зона проведення АТО та окуповані території : аналіт. доп. Київ : НІСД, 2016. 135 с.

СУТНІСТЬ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Кацалап В.О., к.військ.н., доц., Макошенець П.Г.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Враховуючи те, що кіберпростір, це по своїй суті середовище (віртуальний простір) яке надає можливості для здійснення широких комунікацій із значним колом користувачів, першочерговою проблемою є якраз неконтрольований витік інформації (або навпаки вкидання шкідливої інформації чи програм, спаму). Незважаючи на постійне вдосконалення електронних комунікацій, інформаційно-комунікаційних технології, створення нових програм, застосування новітніх програмно-апаратних засобів, витік інформації переважно стається до результатів халатного відношення уповноважених користувачів мережі до заходів безпеки чи цілеспрямованої атаки ворожих суб'єктів з застосуванням сучасніших програм або виявлення прогалин захисту нашого кіберпростору Збройних Сил України [1].

Майже всі ми перебуваємо в єдиному мережевому просторі, і якщо навіть звичайний працівник або військовослужбовець постраждає від будь-якого вірусу, то по цьому ланцюжковій реакції може статися зараження на всіх рівнях. Адже коли майже у кожного існує доступ до мережі Інтернет, особливо актуальним є розмежування використання будь яких програм (додатків) як то під час виконання службових обов'язків так і у вільний від служби час. Необізнаність військовослужбовців та працівників ЗСУ у елементарних алгоритмах дії засобів зв'язку та передачі інформації (комп'ютерів, смартфонів) наносить не поправну шкоду безпеці у віртуальному середовищі, сприяє кібератакам, надає доступ ворожим суб'єктам до інформації, видає за допомогою геолокації місцеположення особового складу та частин, вражає засоби зв'язку шпигунськими програмами. Особливо слід приділити увагу саме на індивідуальне виховання безпечного користування Інтернетом військовослужбовців і працівників ЗСУ, без формального підходу. Так як саме на індивідуальних рисах військовослужбовців і працівників ЗСУ може бути побудована кібератака. Адже слідкуючи за настроями суспільства, новинами, уподобаннями та соціальними мережами, ворожі суб'єкти створюють програми-шпигуни та віруси які потім вдало вражають кіберпростір України.

Для запобігання та вирішення цієї проблеми необхідно постійно проводити діагностування систем шляхом проведення певних тестів, використання спеціалізованого обладнання та залучення кваліфікованих фахівців, здатних усунути причини можливих загроз. Саме тому одним із найважливіших аспектів кібернетичної безпеки є проведення тренінгів з працівниками щодо запобігання та протидії кібератакам. Мають відбуватися постійні навчання та жорсткі інструктажі з користувачами, які своїми ненавмисними діями можуть нанести шкоду державі чи національним інтересам України [2].

При існуючих проблемах кібербезпеки Збройних Сил України, додаткову увагу хочу звернути на міжнародне співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю. Висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею, відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об’єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і незадекларованих функцій у такому обладнанні та звужують вітчизняні спроможності протидії кіберзагрозам. Значна частина підприємств, установ та організацій усіх форм власності не забезпечують кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі. Передумови та чинники, які формують окреслені загрози: недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері, відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом.

Таким чином, основною проблемою кібербезпеки Збройних Сил України є те, що фінансування кіберзахисту здійснюється за залишковим принципом з технологічними помилками. Також велике значення має відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів.

Література
1. Даник Ю., Воробієнко П., Чернега В. Основи кібербезпеки та кібероборони : підручник. Одеса : ОНАЗ, 2018. 228 с.
2. Забезпечення кібербезпеки у ЗС : навч. посіб. / С. А. Микусь та ін. Київ : НУОУ, 2021. 176 с.

МОНІТОРИНГ КОГНІТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Клунник М.С.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Відповідно до основних положень Стратегії інформаційної безпеки України одним з основних шляхів її реалізації є “розробка методологічних підходів оцінювання негативного інформаційно-психологічного впливу в кіберпросторі”. Розвиток Сил оборони України вимагає запровадження універсальних механізмів планування для всієї системи забезпечення інформаційної безпеки. В першу чергу процедур виявлення негативного інформаційного-психологічного впливу, що дозволять синхронізувати інформаційну протидію всіх складових Сектору безпеки та оборони України. Цільові аудиторії у своїй більшості мислять раціонально та використовують доступну їм інформацію, щоб передбачити наслідки своїх дій, перш ніж вони вирішать щось зробити. Після аналізу всіх попередніх досліджень виникла необхідність обґрунтувати модель, яка могла до певної міри передбачати та пояснювати поведінку і соціальну установку цільової аудиторії.

Моніторинг когнітивних інформаційних ресурсів в кіберпросторі передбачає заходи пошуку загроз національній безпеці у сфері оборони (аналіз контенту джерел відкритої інформації, соціальних мереж, месенджерів, віртуальних приватних мереж) [1].

1. Забезпечення безпечного використання кіберпростору:

- створення та розвиток спроможностей Міністерства оборони України та Збройних Сил України щодо забезпечення безпечного використання кіберпростору України в інтересах оборони;
- створення захищеної ІТ-інфраструктури та системи управління державними оборонними ресурсами;
- контроль (моніторинг) стану інформаційної безпеки у сфері оборони в кіберпросторі (виявлення та нейтралізація інформаційних загроз в кіберпросторі);
- контроль (моніторинг) стану кіберзахисту, кібербезпеки, готовності до кібероборони (попередження та нейтралізація кіберзагроз);

- контроль (моніторинг) за виконанням вимог щодо кіберзахисту, кібербезпеки, кібероборони (здійснення аудиту);
- організація захисту персональних даних особового складу Міністерства оборони України та Збройних Сил України;

2. Реагування та допомога з кіберзахисту, кібербезпеки, кібероборони:

- ведення формулярів систем електронної комунікації та баз даних уразливостей програмно-апаратного забезпечення;
- дистанційний контроль (моніторинг) програмних та програмно-апаратних засобів захисту інформації;
- виявлення уразливостей програмного та програмно-апаратного забезпечення та мережевих конфігурацій систем електронної комунікації;
- оперативне управління реагуванням на кіберінциденти та кіберзатаки;
- взаємодія з системою інших відомчих CSIRT, CERT.

Сумісні дії з іншими суб'єктами забезпечення кібербезпеки України:

- щодо боротьби з кібертероризмом;
- щодо боротьби з кіберзлочинністю;
- під час участі в ООС (щодо встановлення спеціального режиму роботи телекомунікаційних засобів).

Організація та проведення відомчих, міжвідомчих та міжнародних кібернавчань (тренувань) персоналу та структурних підрозділів Міністерства оборони України та Збройних Сил України.

Розробка та впровадження спеціальних програмних засобів щодо:

- здійснення моніторингу;
- ведення кіберрозвідки;
- порушення функціонування об'єктів інформаційної інфраструктури;
- здійснення заходів попередження та протидії інформаційним загрозам в кіберпросторі;
- введення противника в оману;
- забезпечення функціонування захищеної системи обміну інформацією та мережі обміну службовою інформацією;
- забезпечення кіберзахисту, кібербезпеки, кібероборони.

Таким чином, моніторинг когнітивних інформаційних ресурсів для забезпечення кібербезпеки дозволяє оцінити в кількісному вимірі рівень інформаційно-психологічного впливу на певну цільову аудиторію за певний проміжок часу в кіберпросторі.

Література

1. Кирило П. Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства Оборони та Збройних Сил України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. Т. 45, № 3. С. 97–100. URL: https://doi.org/10.33099/2311-7249/2022-45-3-97-100.

СУТНІСТЬ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Крищенко А.Є.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

У Збройних Силах України з'явилося розуміння, що таке "кібербезпека", але поки ще, не на всіх ланках є розуміння, для чого потрібен кіберзахист. Не всі розуміють, що система управління Збройних Сил України перебуває в кіберпросторі – основою якого є система зв'язку. А порушення її працездатності призводить до втрати управління військами.

Причиною порушення кібербезпеки може стати, наприклад, слабкий пароль на обладнанні, неправильні налаштування та коригування системи, що може призвести до її зламу. Трапитися це може будь-де у кіберпросторі інформаційно-телекомунікаційної системи Збройних Сил України, у будь-якій військовій частині. Тому головне завдання – передбачити ці події і своєчасно вжити заходів упередження, щоб зменшити ризики [1].

Якщо говорити стратегічно про проблеми кібербезпеки Збройних Сил України, то можливо сказати, що асиметричну відповідь російській федерації могли дати кібервійська, які слід було створити ще на початку гібридної агресії.

Стратегія кібербезпеки України, зокрема, передбачає створення кібервійськ в системі Міністерства оборони України, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору.

Тому, в найближчій перспективі є необхідність створення командування Кібервійськ (Кіберсил), як окремогороду сил Збройних Сил України, що забезпечить цілеспрямоване, взаємоузгоджене виконання завдань кіберрозвідки, кіберзахисту та кібервпливу під єдиним керівництвом.

Кібервійська Збройних Сил України мають бути оснащені сучасними зразками технічних комплексів обробки даних, спеціальними інструментами, технологіями хмарних обчислень та програмними засобами (кіберзброєю). Вони мають бути спроможні виконувати завдання з оборони національного кіберпростору, організації та ведення радіоелектронної (електромагнітної) та кібероборотьби у кіберпросторі або через кіберпростір чи в електромагнітному спектрі [2].

Одною із важливих проблем буде комплектування особовим складом кібервійськ, адже у кібервійська мають входити не просто призовники, а спеціалісти з високим рівнем кваліфікації, підготовки, високим грошовим утриманням, яке відповідатиме ринковим заробітним платам ІТ-спеціалістів.

У зв'язку з цим, в подальшому необхідно буде внесення відповідних змін до законів України.

Таким чином, у найближчій перспективі Збройні Сили України повинні набути та розвивати спроможності із всеохоплюючої ефективної кібербезпеки,

основою якої є використання переваг в електромагнітному середовищі, частиною якого є кіберпростір.

Література

1. Левченко О. В. Еволюція гібридної війни Російської Федерації проти України. *Наука і оборона*. 2017. Т. 2. С. 11–16.
2. Зеленін В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни : навч. посіб. Київ : Люта справа, 2015. 384 с.

АНАЛІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Мілих Є.Г.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Загальні положення щодо забезпечення кібербезпеки України викладені у відповідному Законі України “Про основні засади забезпечення кібербезпеки України”. Одним із основних напрямів забезпечення кібербезпеки України є “забезпечення ефективного застосування Збройних Сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору”.

На мою думку, однією з головних проблем будь-якого державного органу, включаючи Збройні Сили України, є відсутність підготовлених кадрів за напрямом кібербезпеки (“вмотивованих та якісно підготовлених кадрів”, - як зазначає командувач Військ зв’язку та кібербезпеки ЗСУ) матеріально-технічне забезпечення за допомогою країн-партнерів триває та покращується. Так, Європейський Союз створив кіберлабораторію для Збройних Сил України, яка може бути використана для підготовки кадрів, відбиття кібератак та підсилення всієї системи кіберзахисту Збройних Сил України [1].

Ще однією проблемою, з якою стикаються не тільки Збройні Сили України, - це відсутність достатнього правового поля для здійснення діяльності в цій галузі, де б було чітко розмежовано сфери відповідальності суб’єктів забезпечення кібербезпеки. Кіберрозвідка, кіберзахист, активні дії в кіберпросторі є складовими кібербезпеки. Проблемним постає питання здійснення кіберрозвідки та активних дій в кіберпросторі в межах чинного правового поля, яке не визначено для Збройних Сил України.

Ще однією проблемою є те, що на сьогоднішній день створені кіберполігони, але невирішеним є питання їх пов’язання в єдину систему забезпечення кіберзахисту, кібертренувань та кібернавчань на всіх рівнях військового управління Збройних Сил України [2].

Майже два роки тому було створено нове Командування військ зв'язку та кібернетичної безпеки Збройних Сил України. Існує гостра необхідність розмежування двох напрямів: а саме забезпечення зв'язку та кібернетичної безпеки, як це існує в провідних країнах світу. Варто зауважити, що система управління Збройних Сил України перебуває в кіберпросторі, але не всі повністю усвідомлюють важливість цього.

Питання, яке потребує звернення уваги, - це питання рівня кіберграмотності військовослужбовців.

Отже, очевидним є важливість питання забезпечення кібербезпеки для держави в цілому та для Збройних Сил України зокрема. Напрям розвитку є доволі новим, тому існує низка питань, які потребують нагального вирішення.

Література

1. Даник Ю., Воробієнко П., Чернега В. Основи кібербезпеки та кібероборони : підручник. Одеса : ОНАЗ, 2018. 228 с.
2. Бабич Є. Ю. Забезпечення кібербезпеки в Україні : thesis. 2016. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/5102.

ФАКТОРИ, ЯКІ ВПЛИВАЮТЬ НА СТАН КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Оніщук В.С.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

У сучасному суспільстві кібератаки стають частішими та мають тенденцію чинити все значніший і триваліший вплив на економіку країни, незаперечним є той факт, що надійний захист від кібератак активно впливає на стан економічної, політичної, соціальної, оборонної та інших складових національної безпеки держави [1].

Очевидним є той факт, що порушення функціонування об'єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великого матеріального, фінансового, економічного збитку або великомасштабними порушеннями життєдіяльності міст та населених пунктів. У цих умовах надзвичайно важливу роль відіграє забезпечення безпеки, у тому числі і кібербезпеки об'єктів критичної інфраструктури держави [2].

Враховуючи зазначене вище, метою тез є визначення основних факторів, що впливають на стан кібербезпеки об'єктів критичної інфраструктури.

Проведений аналіз існуючих систем захисту інформації, дає змогу визначити основні складові частини системи кіберзахисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури:

- нормативно-правова;
- організаційна;
- технічна;
- підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки ІТС ОКІ.

ІТС зазвичай являються об’єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об’єкти захисту від кіберзагроз.

Відповідно проведеного аналізу, на стан забезпечення кібербезпеки ІТС об’єкта критичної інфраструктури можуть впливають такі фактори:

- наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки ІТС об’єктів критичної інфраструктури;
- наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;
- наявність вразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак.

Також, одним із таких показників може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.

Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, об’єкти сектору безпеки і оборони, відомства, дипломатичні установи тощо.

Таким чином, кібербезпека є невід'ємною складовою інформаційної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної та інформаційно-технологічної безпеки держави.

Література

1. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько та ін. *Системи управління, навігації та зв'язку*. 2016. Т. 4, № 40. С. 81–84.
2. Гук О. М. Дії в кіберпросторі під час підготовки та ведення мережецентричної війни. *Науковий журнал Сучасні інформаційні технології у сфері безпеки та оборони*. 2017. Т. 2, № 29. С. 107–111.

ПРОБЛЕМИ РОЗВИТКУ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Перегуда С.П.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Питання кібернетичної безпеки, а особливо в зоні проведення бойових дій, сьогодні дуже гостро стоїть в Збройних силах України. Нині склалася така ситуація, коли переважна більшість людей, залучених до захисту держави, включаючи офіцерів, сержантів, солдат не усвідомлюють небезпеки і можливих наслідків протистояння у площині кіберпростору [1].

Одна з головних проблем кібербезпеки Збройних Сил України є нехтування правилами, такими як:

- вимкнене геопозиціонування або визначення місця перебування на усіх пристроях;
- оновлення антивірусу;
- застосування сильних паролів;
- використання WiFi-роутерів та інтерет модемів;
- дотримання правил поведінки в соціальних мережах.

Наступна проблема кібербезпеки Збройних Сил України є низька обізнаність та підготовка особового складу, що призводить до:

- помилки при проектуванні та розробці програмного програмно-апаратного забезпечення;
- навмисні дії по внесенню вразливостей в ході проектування і розробки програмного програмно-апаратного забезпечення;
- неправильні налаштування програмного забезпечення, неправомірна зміна режимів роботи пристроїв та програм;
- несанкціоноване впровадження і використання неврахованих програм з подальшим необґрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);
- впровадження шкідливих програм, що створюють уразливості в програмному і програмно-апаратному забезпеченні;
- несанкціоновані ненавмисні дії користувачів, що призводять до виникнення дефектів;
- збої в роботі апаратного і програмного забезпечення (викликані збоями в електроживленні, виходом з ладу апаратних елементів у результаті старіння і зниження надійності, зовнішніми впливами електромагнітних полів технічних пристроїв).
- уразливості системного програмного забезпечення (у тому числі протоколів мережного взаємодії);
- уразливості прикладного програмного забезпечення (у тому числі засобів захисту інформації) [2].

Отже, для Збройних Сил України залишається актуальною низка проблемних питань кібербезпеки, вирішення яких потребуватиме часу та зусиль як з боку командирів (начальників), так і з боку підлеглого особового складу. Від ефективності їх вирішення залежить, якою мірою Збройних Сил України зможуть відповідати на сучасні кібербезпекові виклики.

Література

1. Про деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку: Постанова Кабінету Міністрів України № 303 від 14 травня 2015 р. База даних "Законодавство України" / ВР України. URL:http//zacon2.rada.gov.ua/laws/show.
2. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України № 1009 від 06 грудня 2017 р. База даних "Законодавство України" / ВР України. URL:http//zacon2.rada.gov.ua/laws/show.

СИТУАЦІЙНИЙ АНАЛІЗ КІБЕРБЕЗПЕКИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Сичов О.Л.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Система кібербезпеки Міністерства оборони України та Збройних Сил України є однією із складових системи забезпечення інформаційної безпеки держави у воєнній сфері яка може діяти автономно, як основний механізм формування інформаційних ресурсів для реалізації процесів управління Збройними Силами України. Тому процес обґрунтування вимог до кібербезпеки Міністерства оборони України є основною її проблемою яка безпосередньо залежати від умов її функціонування, зокрема доступності та захищеності необхідних інформаційних ресурсів [1].

Склад та характеристики основних показників. Система може оперативно реагувати на кіберзагрози в умовах широкомасштабної війни:

- гарантованого виявлення кіберзагроз та об'єктів їх впливу;
- ідентифікації виявлених об'єктів інформаційного впливу;
- надання варіантів протидії на виявлення кіберзагроз;
- видачі інформації визначеним споживачам.

Відповідно до функціонального призначення Система має виконувати наступні завдання:

- ведення розвідки у навколишньому просторі для виявлення об'єктів інформаційного впливу противника;

- формування інформації про діяльність інформаційних об’єктів противника;
- визначення ознак інформаційного впливу противника;
- класифікація виявлених інформаційних об’єктів противника;
- прогнозування можливих наслідків діяльності інформаційних об’єктів противника;
- видача інформації особі приймаючій рішення для протидії інформаційному впливу противника;
- управління елементами Системи;
- здійснення об’єктивного контролю результатів бойової роботи Системи.

Окремі елементи Системи можуть бути використані як локальні джерела інформації, а також з метою проведення заходів з оцінки спроможностей, навчань та підготовки особового складу [2, 3].

Особливості взаємодії. Система взаємодіє з іншими інформаційними системами держави та ЗС України, а також споживачами інформації реального часу через уніфікований стик з Єдиною АСУ ЗС України.

Викладені основні вимоги до системи інформаційних заходів в інтересах запобігання виникнення воєнних конфліктів, для запровадження державної системи забезпечення інформаційної безпеки, зокрема у воєнній сфері, та реалізація доцільного варіанту її організаційної структури відкриває можливий шлях до ефективного управління процесом забезпечення кібербезпеки Міністерства оборони України та Збройних Сил України.

Основними вимогами до системи кібербезпеки Міністерства оборони України та Збройних Сил України:

- системна організація кіберзаходів;
- взаємодія з центральними органами виконавчої влади, іншими військовими формуваннями та правоохоронними органами, обласними та районними державними адміністраціями, неурядовими громадськими організаціями;
- забезпечення кіберпідтримки дій військ (сил) Збройних Сил України в єдиній системі заходів реалізації державної інформаційної політики;
- чітка координація кіберзаходів в єдиній системі;
- забезпечення цілодобового моніторингу кіберпростору в інтересах оборони України;
- формування інтегрованої системи виявлення, оцінювання та реагування на кіберзагрози;
- використання всіх можливостей Міністерства оборони України та Збройних Сил України;
- створення необхідних умов для підвищення ефективності інформаційних заходів.

Таким чином, наведений ситуаційний аналіз кібербезпеки Міністерства оборони України показав, що існуюча суб’єкти кібербезпеки постійно функціонує в різних умовах. Це впливає на її можливість реалізовувати свої

спроможності в різноманітних умовах, як на етапі планування, так і безпосередньо ведення кібероборони держави.

Література

1. Ruan K. Introducing cybernomics: a unifying economic framework for measuring cyber risk. *Computers & security*. 2017. Vol. 65. P. 77–89. URL: https://doi.org/10.1016/j.cose.2016.10.009 (date of access: 30.03.2023).
2. Borghard E. D., Lonergan S. W. Can states calculate the risks of using cyber proxies?. *Orbis*. 2016. Vol. 60, no. 3. P. 395–416. URL: https://doi.org/10.1016/j.orbis.2016.05.009 (date of access: 30.03.2023).
3. Srinivas J., Das A. K., Kumar N. Government regulations in cyber security: framework, standards and recommendations. *Future generation computer systems*. 2019. Vol. 92. P. 178–188. URL: https://doi.org/10.1016/j.future.2018.09.063 (date of access: 30.03.2023).

АНАЛІЗ КІБЕРЗАГРОЗ ФУНКЦІОНУВАННЮ ЗБРОЙНИХ СИЛ УКРАЇНИ

Соловйов Е.П.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

На сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від безперешкодного функціонування п’ятого простору – кіберпростору, під яким пропонується розглядати сукупність взаємопов’язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп’ютерних мережах і пов’язаній з ними інфраструктурі, разом з об’єктами, що підпадають під їх контроль та управління.

Захист інтересів держав та громадян в кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання ІТ-мереж на питання безпеки й оборони. Потенційна небезпека може загрожувати системам державного та військового управління, економіки та промисловості.

Україна інтегрована у світовий кіберпростір і відповідно зазнає різних загроз і негативних впливів, пов’язаних з його розвитком (зокрема від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов’язаних із розбудовою національної системи кібербезпеки.

Питання кібернетичних загроз та кібернетичного захисту гостро стоїть у військовій сфері, з причини того, що управління військами, зв'язок, а також складова суспільної інформаційної боротьби стала невід'ємною складовою повсякденного життя ЗС України в умовах широкомасштабної війни.

Використання програмного забезпечення з відкритим кодом несе за собою відповідальність за впровадження даного елементу в ІТС ЗС України. Адже програмне забезпечення містить велику кількість бекдорів та закладок, які можуть надавати доступ зловмисникам до програмних продуктів, та отримувати інформацію, що проходить через них [1].

Проте на практиці використання такого обладнання дає змогу побудувати мережевий міст на відстань лише до 10 кілометрів, за умови прямого бачення. Та навіть такі технічні характеристики дають змогу виявити деякі критичні вразливості в даному обладнанні та використати їх для реалізації кібернетичних атак зокрема впровадження атаки всередині (інсайдерства).

Визначення наявних загроз кібернетичній безпеці, є одним з початкових етапів на шляху створення та вдосконалення наявної системи забезпечення кібернетичної безпеки в ІТС ЗС України. В рамках написання цієї роботи було проведено аналіз сегменту кібернетичного впливу в ІТС ЗС України. Визначено, що основним сегментом ІТС ЗС України є ВЗ. Основними об'єктами захисту є: маршрутизатори, сервери, телекомунікаційне обладнання та користувачі ІТС. Розглянуто основні засоби для забезпечення кібернетичного захисту, та поняття кібернетичного захисту згідно наявного законодавства в галузі кібернетичної безпеки.

Література

1. Мордюк А. О. Як працювати з інтернет-контентом, щоб не стати жертвою маніпуляції: поради журналістам від вітчизняних та європейських експертів. *Наукові записки Інституту журналістики*. 2014. Т. 56. С. 240–246.

ПРОЦЕС УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕТОДИ ЇХ ОЦІНКИ

Наумов В.І.
Державний університет телекомунікацій
м.Київ, Україна

Актуальність управління ризиками обумовлюється тим, що ризики притаманні будь-якій організації та пов'язані з використанням її інформаційних систем, які підтримують місію організації та її бізнес-функцій.

З точки зору інформаційної безпеки ризик можна розглядати як можливість понести втрати через порушення конфіденційності, цілісності, автентичності або доступності інформаційних активів, які представляють цінність для організації та потребують захисту, внаслідок цільових кібератак,

технічних збоїв, недбалості та необізнаності персоналу. Ризики інформаційної безпеки вважаються частиною бізнес-ризиків і розглядаються подібним чином. Оцінка ризиків інформаційної безпеки починається з вивчення інформаційних систем, визначення інформаційних активів і опису технології обробки інформації [1].

Основою для впровадження процесу управління ризиками є міжнародні стандарти ISO/IEC 27005 та ISO 31000, які містять настанови щодо управління ризиками ІБ та загальними бізнес-ризиками відповідно [2]. Відповідно до цих стандартів, процес ризик-менеджменту є ітеративним та складається з таких кроків:

- Встановити контекст управління ризиками;
- Оцінити та обробити інформаційні ризики;
- Моніторити та переглядати ризики, критерії ризиків на постійній основі.

Також стандарт ISO 31000:2018 висуває декілька рекомендацій щодо принципів процесу управління ризиками, яких має слідувати організація, яка бажає ефективно впровадити даний процес. Так, процес ризик-менеджменту повинен бути [3]:

- Інтегрований – управління ризиками має бути невід'ємною частиною діяльності організації;
- Структурований і всеосяжний – структурований і комплексний підхід до управління ризиками дає послідовні та порівнювані результати;
- З можливістю адаптації – структури та процеси управління ризиками взаємопов'язані та адаптовані з урахуванням зовнішнього та внутрішнього середовища організації, що відповідає її завданням;
- Динамічний – ризики можуть виникати, змінюватися або зникати, коли змінюється зовнішнє та внутрішнє середовище організації. Управління ризиками передбачає, виявляє, ідентифікує та реагує на ці зміни та події належним і своєчасним чином;
- Постійно вдосконалюваним – необхідно постійно вдосконалювати процес управління ризиками через навчання та досвід.

Як вже було вказано раніше, ризики притаманні будь-якій організації та можуть призвести до певних видів збитків, серед яких можна виділити:

1. Економічні втрати;
2. Втрата репутації;
3. Збитки внаслідок порушення законів або контрактів;
4. Загрози продуктивності праці працівників;
5. Загроза життю та здоров'ю людей.

Економічний збиток можна точно оцінити за допомогою наведених вище типів збитків. Зменшення продуктивності та втрати персоналу через порушення законів чи контрактів можна обчислити в менш точних грошових виразах, оскільки реалізація певних ризиків потребує не лише економічних санкцій, а й економічно неоціненних санкцій (кримінальна відповідальність, відкликання ліцензій) тощо. Шкода репутації та загроза життю та здоров'ю людей не підлягають економічній оцінці. Імовірність реалізації ризику неможливо точно

оцінити. Подібні дані про випадки з державних установ, CERT та галузевих асоціацій можна використовувати як джерело інформації про ймовірність виникнення ризику. Однак усі ці дані часто є неточними (багато компаній не розкривають подробиці інцидентів інформаційної безпеки), неповними (не всі компанії контролюються), нерелевантними. Крім того, ці цифри не враховують специфіку конкретної компанії. Тому статистика інцидентів інформаційної безпеки, що відбулися, враховується в оцінці ризику, але її слід використовувати з обережністю. Оскільки ані втрати, ані ймовірність неможливо визначити кількісно, величину ризику неможливо розрахувати за визначенням. З цією метою було прийнято підхід до оцінки ризиків на основі якісних показників. Найпростіший метод, як визначено в Керівництві з оцінки ризиків NIST SP 800-30 або методології оцінки ризиків OWASP, передбачає оцінку ступеня небезпеки та ймовірності реалізації ризику за якісною шкалою (низький/помірний/високий) і на основі це згідно з таблицею різновидів ризику. Різниця полягає лише в кількості рівнів класифікації та правилах, які визначають віднесення рівня збитків та ймовірності реалізації ризику до того чи іншого.

Література

1. Ризик (інформаційна безпека). 2022. URL: https://www.wiki-data.uk-ua.nina.az/Ризик_(інформаційна_безпека).html
2. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)
3. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT)

АНАЛІЗ ПІДХОДІВ ЩОДО ПІДГОТОВКИ ТА ВЕДЕННЯ КІБЕРОБОРОНИ ДЕРЖАВИ

Томашевський О.С.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

В сучасному світі питання кібербезпеки та кібероборони стали наріжними і найбільш проблемними та актуальними в забезпеченні національної безпеки і оборони практично всіх розвинених держав. На саміті НАТО в Варшаві (7-9.07.2016) на Кіберконференції з інформаційного забезпечення НАТО (NIAS) (6.12.2016), на конференції “Кібернетична оборона” (Париж, 15.05.2018), на засіданні Північноатлантичної ради (Брюссель 11 12.07.2018) та на саміті у Лондоні у листопаді 2019 року присвяченому 70-річчю створення альянсу НАТО було зосереджено увагу на важливості своєчасного виявлення, запобігання, нейтралізації і ліквідації загроз в кіберпросторі [1, 2].

Отже, аналіз та узагальнення відомих результатів досліджень, розвиток та

практична реалізація виконання завдань суб'єктами забезпечення кібербезпеки та кібероборони держави провідних країн світу надасть можливість визначити основні підходи щодо підготовки та ведення кібероборони нашої держави.

Питання та передумови виникнення напрямів кібербезпеки та кібероборони в тому чи іншому контексті пов'язані із появою та розвитком радіотехніки і радіоелектроніки, електронної техніки і технічних засобів шифрування та криптоаналізу, обчислювальної техніки і інформатики, кібернетики, теорії зв'язку та інформації, стрімким розвитком інформаційно-телекомунікаційних такіберсистем, їх впровадженням в усі галузі й сфери людської діяльності.

Однією з перших країн, яка на державному рівні висвітила кібербезпеку як окремий вид безпеки, були США. У лютому 2003 р. у США була оприлюднена "Національна стратегія щодо забезпечення безпеки кіберпростору" (National Strategy to Secure Cyberspace), в якій були визначені об'єкти критичної кіберінфраструктури, що підлягають кіберзахисту, а саме: державні та приватні установи різних галузей господарства, промисловості, уряду, оборонного комплексу, телекомунікацій, енергетики, транспорту, банківської справи та фінансового сектору, хімічної промисловості та виробництва небезпечних речовин, судноплавства.

Нові вразливості національної критичної інфраструктури, які проявляються паралельно з бурхливим розвитком технологій, породжують нові небезпеки, загрози й ризики в інформаційному та кіберпросторах та вимагають вирішення питань щодо їх запобігання, стримування та нейтралізації.

Виходячи з цього, у держав виникає необхідність утворення ефективної системи кібербезпеки та кібероборони з функціональною спроможністю не нижче гранично необхідного рівня, не залежно від рівня їх економічного розвитку і стану та науково-технічного прогресу країни, але адекватно до рівня загроз, що притаманні світові у першій чверті XXI століття, а у стратегічній перспективі – до середини століття [2].

Таким чином, аналіз підходів щодо підготовки та ведення кібероборони держави показав, що особливістю кібероборони є необхідність захисту кіберсистем об'єктів критичної інфраструктури свого сектору національної безпеки та оборони, військового управління, комплексів озброєння та військової техніки, а також досягнення необхідних спроможностей деструктивного впливу на ІТС противника.

Література

1. Network centric warfare market | industry analysis and market forecast to 2021. *MarketsandMarkets*. URL: https://www.marketsandmarkets.com/Market-Reports/network-centric-warfare-market-77370144.html.
2. BMC4ISR - battle management/command, control, communications, computers, intelligence, surveillance, and reconnaissance | acronymfinder. *Abbreviations and acronyms dictionary*. URL: https://www.acronymfinder.com/Battle-Management/Command,-Control,-

Communications,-Computers,-Intelligence,-Surveillance,-and-Reconnaissance-(BMC4ISR).html.

СУЧАСНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Шайхет С.О., к.н.держ.упр.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

Стрімкий розвиток та масове впровадження досягнень електроніки, сучасних інформаційних та кібер- технологій призвели до формування нового спектру ризиків та загроз у сфері національної безпеки і оборони держави, які реалізуються у кіберпросторі та (або) через кіберпростір. Відбувається стрімке зростання інформатизації та автоматизації всіх сфер людської діяльності, кількості інформації, що зберігається, обробляється і передається, швидкості її передачі і обробки, ускладнення систем управління, взаємодії між ними і зв'язків між процесами управління. Кіберзагрози охоплюють всі базові сфери суспільної діяльності (політичну, військову, правову, економічну, енергетичну, соціальну духовну, технологічну) [1].

За останнє десятиліття кіберпростір став п'ятою окремою, специфічною та важливою сферою ведення збройної боротьби, поряд із чотирма традиційними – "Земля", "Море", "Повітря" та "Космос". Нині вже буденним сприймається застосування державами кібервійськ та кіберзброї, здійснення кібероборони, кібероперацій та кібератак.

У Законі України "Про основні засади забезпечення кібербезпеки України" вперше законодавчо визначено такі терміни:

- кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;
- кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
- кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

У Збройних Силах України з'явилося розуміння, що таке "кібербезпека",

але поки ще, не на всіх ланках є розуміння, для чого потрібен кіберзахист. Не всі розуміють, що система управління Збройних Сил України перебуває в кіберпросторі – основою якого є система зв'язку [2].

Дуже велика небезпека в користуванні нашими військовослужбовцями мобільних телефонів – як під час перебування у пункті постійної дислокації, так і в районі проведення бойових дій. Будь-який мобільний телефон – це радіозасіб, який можна запеленгувати. Противник може визначити і відстежити скупчення мобільних телефонів, що є розвід-ознакою, і завдати вогневого ураження або інформаційного – наприклад, зробити смс-розсилку повідомлень деморалізуючого характеру.

Причиною порушення кібербезпеки може стати, наприклад, слабкий пароль на обладнанні, неправильні налаштування та коригування системи, що може призвести до її зламу. Трапитися це може будь-де у кіберпросторі інформаційно-телекомунікаційної системи Збройних Сил України, у будь-якій військовій частині. Тому головне завдання – передбачити ці події і своєчасно вжити заходів упередження, щоб зменшити ризики.

Якщо говорити стратегічно про проблеми кібербезпеки Збройних Сил України, то можливо сказати, що асиметричну відповідь російській федерації могли дати кібервійська, які слід було створити ще на початку гібридної агресії.

Також, комплексне виконання завдань в електромагнітному та кіберпросторі вимагає інтеграції в єдину систему сил і засобів радіоелектронної та кіберборотьби.

Стратегія кібербезпеки України, зокрема, передбачає створення кібервійськ в системі Міністерства оборони України, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору.

Тому, в найближчій перспективі є необхідність створення командування Кібервійськ (Кіберсил), як окремого роду сил Збройних Сил України, що забезпечить цілеспрямоване, взаємоузгоджене виконання завдань кіберрозвідки, кіберзахисту та кібервпливу під єдиним керівництвом.

Кібервійська Збройних Сил України мають бути оснащені сучасними зразками технічних комплексів обробки даних, спеціальними інструментами, технологіями хмарних обчислень та програмними засобами (кіберзброєю). Вони мають бути спроможні виконувати завдання з оборони національного кіберпростору, організації та ведення радіоелектронної (електромагнітної) та кіберборотьби у кіберпросторі.

Одною із важливих проблем буде комплектування особовим складом кібервійськ, адже у кібервійська мають входити не просто призовники, а спеціалісти з високим рівнем кваліфікації, підготовки, високим грошовим утриманням, яке відповідатиме ринковим заробітним платам ІТ-спеціалістів.

Таким чином, перспективі Збройні Сили України повинні набути та розвивати спроможності із всеохоплюючої ефективної оборони на всіх операційних напрямках та в усіх вимірах: наземному, морському, повітряному, космічному та кібернетичному, створити та використовувати переваги в

електромагнітному середовищі, частиною якого є кіберпростір.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави" : Указ Президента України від 26.08.2021 р. № 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (дата звернення: 30.03.2023).
2. Army publishing directorate. *Army Publishing Directorate*. URL: https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1022713.

МЕТОД ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМИ ВИЯВЛЕННЯ, ТА РОСПІЗНАВАННЯ РАДІОСИГНАЛІВ

Собчук В.В., д.т.н., Лаптєва Т.О. аспірантка
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

Під завадою радіосигналу в роботі розуміється будь-який вид електричних коливань, який, проникаючи в радіоприймальні пристрої із зовні або виникаючи всередині його, ускладнює визначення радіосигналу. Сигнал і завада, одночасно діють на вході приймача, відтворюються на виході останнього у вигляді випадкового коливального процесу. В результаті цього неможливо точно визначити параметри сигналу. Нормальне визначення сигналу можливо тільки при певному співвідношенні потужності сигналу і завади на виході приймача [1]. Найменша потужність сигналу, при якій забезпечується задовільне визначення сигналу, залежить від рівня завад. Ця величина потужності характеризує чутливість приймача. Здатність радіоприймального пристрою приймати із заданою якістю сигнал при наявності завад називається завадостійкістю [2]. Покращення завадостійкості радіоприймальних пристроїв – одна з основних і найскладніших проблем радіотехніки . Для успішного вирішення її необхідно вивчити властивості та характер впливу завад на сигнал, а потім визначити способи ослаблення їх впливу на якість визначення сигналу.

Питання подолання завад мають свої особливості і у процесі виявлення та розпізнавання цифрового сингалу радіоефіру. З цією метою розглянемо питання завадостійкості при дослідженні вищезазначених процесів.

Практично усі методи завадостійкості приймання сигналів засновані на принципі усереднення сигналу та завади. Даний принцип полягає у тому, що виконується процес підсумовування. При чому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно. З метою усереднення корисного сигналу та завади застосовуються лінійні системи двох типів: вузькосмугові

фільтри та фільтри низької частоти. При цьому можливо оптимізувати фільтри низької частоти або вузькосмугові фільтри.

Для розгляду питання фільтрації завад, зробимо припущення, що сам вузькосмуговий фільтр не вносить спотворення в форму сигналу, який пройшов через нього. Ідеальний смуговий фільтр – це фільтр з амплітудно-частотною характеристикою виду:

$$K(\omega)=\begin{cases}1 \quad якщо \quad \omega_0-\dfrac{\Delta\omega}{2}\le|\omega|\le\omega_0+\dfrac{\Delta\omega}{2}\\ 0 \quad якщо \quad \left]-\infty,\omega_0-\dfrac{\Delta\omega}{2}\right[U\left]\omega_0+\dfrac{\Delta\omega}{2},\infty\right[\end{cases}, \tag{1}$$

де $\Delta\omega$ – полоса пропускання фільтру.

Для ідеального фільтру ефективна полоса $\Delta\omega_e$ та полоса на рівні $0,707-\Delta\omega_{\sqrt{2}}$, що дорівнює полосі прозорості фільтру $\Delta\omega$.

Для фільтрів вірним є припущення, що $\Delta\omega << \Delta\omega_0$.

Частотна характеристика виразу для (1), це імпульсна перехідна характеристика, яка буде визначатися виразом:

$$h_\delta(t)=\frac{\Delta\omega}{\pi}\cdot\frac{\sin\dfrac{\Delta\omega t}{2}}{\dfrac{\Delta\omega t}{2}}\cos\omega_0 t\ . \tag{2}$$

З огляду на те, що цифрових сигнал не є чітким імпульсом [3], то можна обчислити огинаючу напруги на виході ідеального фільтра при впливі на нього прямокутного імпульсу тривалістю T:

$$x(t)=\begin{cases}X_m\cos\omega_0 t \quad якщо \quad 0\le t\le T\\ 0 \quad якщо \quad \left]-\infty,0\right[U\left]T,\infty\right[\end{cases}, \tag{3}$$

де X_m – огинаюча сигналу $x(t)$ на вході фільтру.

За допомоги теореми про огинаючу напруги вузькосмугового фільтру, запишемо вираз для огинаючою напруги на виході фільтру:

$$Y_m(t)=\frac{1}{2\pi}\int_{-\infty}^{\infty}K_{fn}(j\omega)S_{X_m}(j\omega)e^{j\omega t}dt, \tag{4}$$

де $S_{X_m}(j\omega)=\int_{-\infty}^{\infty}X_m e^{-j\omega t}dt$ – амплітудний спектр огинаючої сигналу $x(t)$,

K_{fn} – комплексний коефіцієнт передачі фільтра низької частоти:

$$K_{fn}(j\omega)=\begin{cases}1 \quad якщо \quad -\dfrac{\Delta\omega}{2}\le|\omega|\le\dfrac{\Delta\omega}{2}\\ 0 \quad якщо \quad \left]-\infty,\dfrac{\Delta\omega}{2}\right[U\left]\dfrac{\Delta\omega}{2},\infty\right[\end{cases} \tag{5}$$

Якщо підставити вираз (5) у вираз (4), то отримаємо вираз:

$$Y_m(t)=\frac{X_m}{2\pi}\big(Si(\Delta\omega t)-Si(\Delta\omega(t-T))\big), \tag{6}$$

де $Si(z)=\int_0^z \frac{\sin t}{t} dt$ – інтегральний синус [4].

На рис. 1 приведено графіки залежності тривалості впливаючого прямокутного імпульсу (влакитний колір – тривалість імпульсу T=1, червоний колір – T=10, зелений колір –T=15 та чорний колір – T=20) від діапазону частоти (полоси пропускання фільтру).

З наведених на рис. 1 графіків бачимо суттєві відмінності вхідного прямокутного імпульсу від вихідного сигналу. Спотворення вхідного імпульсу зростає при збільшення його тривалості. Це спотворення форми імпульсу можливо охарактеризувати співвідношенням тривалості фронту огинаючої імпульсу на виходи фільтра до тривалості огинаючої вихідного імпульсу.

Це свідчить про те, що короткочасні прямокутні сигнали можливо виділяти за допомогою смугового фільтру [5].

Таким чином з метою підвищення завадостійкості системи визначення та розпізнавання , потрібним є використання фільтра низьких частот. За допомогою цього значно понижуються або зовсім виключаються з аналізу завади низьких частот.

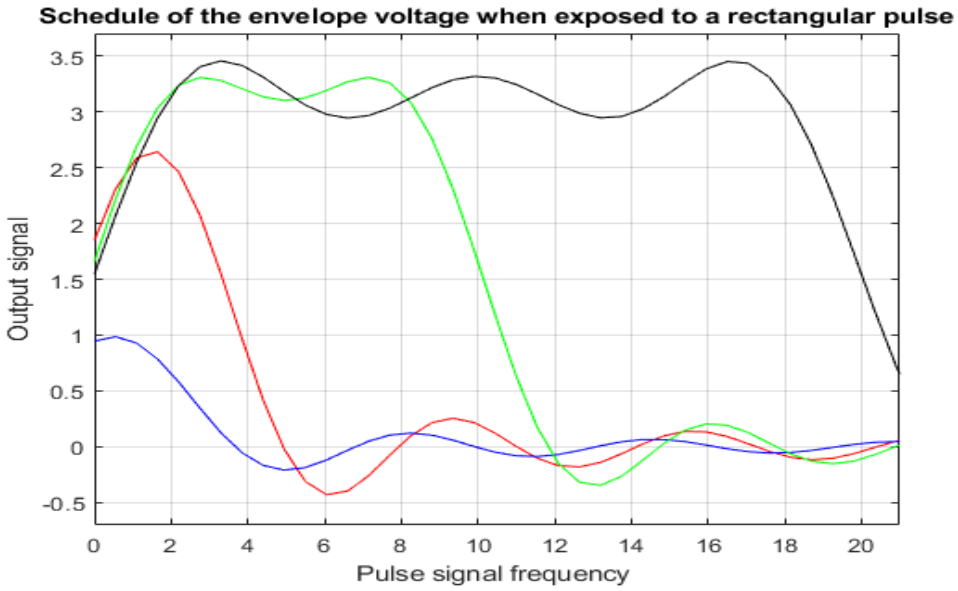


Рис.1. Графік огинаючої напруги при впливі прямокутного імпульсу сигналу

Аналіз напрямків розвитку сучасних засобів негласного отримання інформації показують тенденції переходу їх роботи у діапазон високих частот. Тобто сигнал передачі інформації зміщується у діапазон високих частот, у якому процес визначення та розпізнавання цифрових сигналів є доволі складним.

Виключивши з аналізу завади нижніх частот ми вже значно підвищимо завадостійкість системи у цілому.

Висновки.

Досліджено особливості використання фільтрів низьких частот з метою підвищення завадостійкості автоматизованої системи визначення та розпізнавання цифрових засобів радіоефіру. Показано, що принцип роботи

фільтрів полягає у тому що виконується процес підсумовування. При цьому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно. Тобто при підсумовуванні корисний сигнал збільшується, а сигнал завади зменшується.

Доведено, що використання у процесі обробки сигналів вузько-смугових фільтрів низької частоти дозволяє досягти підвищення завадостійкості системи визначення та розпізнавання цифрових сигналів радіоефіру на 18 %.

Література

1. Functionally sustainable wireless sensor network technologies aspects analysis / A. V. Sobchuk et al. *Science and education a new dimension*. 2019. Vol. VII(193), no. 23. P. 46–48. URL: https://doi.org/10.31174/send-nt2019-193vii23-11 (date of access: 30.03.2023).
2. Лаптєв О.А., Собчук В.В., Савченко В.А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах.*Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. ВІКНУ, 2019. № 66. – С. 90 – 104.
3. Improving the method of searching digital illegal means obtaining information based on cluster analysis / O. Laptiev et al. *Scientific journal of astana IT university*. 2020. No. 3. P. 63–70. URL: https://doi.org/10.37943/aitu.2020.99.72.006 (date of access: 30.03.2023).
4. Oleksandr L. The method of hidden transmitters detection based on the differential transformation model. *International journal of advanced trends in computer science and engineering*. 2019. Vol. 8, no. 6. P. 2840–2846. URL: https://doi.org/10.30534/ijatcse/2019/26862019 (date of access: 30.03.2023).
5. Laptev O., Sobchuk V., Savchenko V. A method of increasing the immunity of a system for detecting, recognizing and localizing digital signals in the information systems. *Collection of scientific works of the military institute of kyiv national taras shevchenko university*. 2019. No. 66. P. 90–104. URL: https://doi.org/10.17721/2519-481x/2020/66-09 (date of access: 30.03.2023).

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Добровольський Д. І.
Державний університет телекомунікацій
м. Київ, Україна

Зростання кількості кібератак сприяє зростанню ринку засобів безпеки на основі ШІ (штучного інтелекту). У звіті Acumen Research and Consulting за липень 2022 року повідомляють, що світовий ринок становив 14,9 мільярда доларів у 2021 році та, за оцінками, досягне 133,8 мільярда доларів до 2030 року[1].

З кожним роком накопичується велика кількість даних через зростання IoT (Інтернету речей), хмарного сховища та збільшення кількості користувачів Інтернету. Важко зберігати великий обсяг даних, водночас, зберігаючи конфіденційність.

Використання штучного інтелекту в управлінні інформаційною безпекою може забезпечити більш ефективне виявлення та запобігання кібератакам та іншим загрозам безпеці.

Однак, використання ШІ також створює нові задачі, пов'язані з конфіденційністю даних, алгоритмічною упередженістю та відповідальністю за прийняття рішень, що можуть поставити під загрозу безпеку даних та приватність користувачів.

Проблема полягає у тому, що штучний інтелект може призвести до того, що вирішення проблем інформаційної безпеки будуть здійснюватися автоматично без достатньої людської оцінки, що може призвести до небажаних наслідків.

Крім того, наявність алгоритмічної упередженості у системах ШІ може спричинити некоректне прийняття рішень, що також може стати проблемою для безпеки даних отож, розумним рішенням буде створити механізми для виявлення та виправлення алгоритмічної упередженості, що можуть допомогти знизити ризики для безпеки даних та приватності користувачів.

Для рішення цих проблем, важливо забезпечити ефективний нагляд та контроль за системами ШІ, а також розробити технічні та правові рішення, що забезпечать конфіденційність даних та відповідальність за прийняття рішень.

Створення механізмів для виявлення та виправлення алгоритмічної упередженості є складним та комплексним завданням, оскільки ця проблема пов'язана з проблемами, які виникають в процесі розробки, навчання та тестування алгоритмів штучного інтелекту. Проте, існують деякі можливі підходи до створення механізмів виявлення та виправлення алгоритмічної упередженості, зокрема:

- Забезпечення розширеної розподіленої бази даних:

Цей підхід передбачає розширення баз даних, використовуваних для навчання ШІ, з метою збільшення кількості даних, які використовуються для навчання. Це допомагає знизити ризики алгоритмічної упередженості, оскільки збільшення кількості даних може знизити ризики зведення алгоритмів до стереотипів.

- Моніторинг та перевірка алгоритмів:

Цей підхід включає моніторинг та перевірку алгоритмів ШІ з метою виявлення відхилень та упередженостей у вирішенні завдань. Це може бути досягнуто за допомогою валідації алгоритмів на тестових даних, порівняння алгоритмів зі стандартними методами розв'язання задач, або шляхом перевірки на відповідність етичним та правовим вимогам.

- Використання технік зменшення упередженості:

Цей підхід включає застосування технік зменшення упередженості, таких як збалансоване навчання та зменшення ваги атрибутів, які можуть спричиняти

упередження, у процесі навчання ШІ. Також є сенс використовувати методи інтерпретації алгоритмів, що дозволять зрозуміти, як саме приймаються рішення системою ШІ та виявити можливі проблеми з алгоритмічною упередженістю.

Усі ці методи можуть бути поєднані для створення ефективного механізму для виявлення та виправлення алгоритмічної упередженості, що забезпечить безпеку даних та приватності користувачів у системах ШІ.

Таким чином, використання штучного інтелекту в управлінні інформаційною безпекою має великий потенціал, але вимагає ретельного планування та розробки. Для успішного впровадження ШІ у системи управління інформаційною безпекою необхідно вирішити складні проблеми з дотриманням конфіденційності даних, алгоритмічною упередженістю та людським контролем.

Література

1. Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most URL: https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html]

БЕЗПЕКА ФУНКЦІОНУЮЧИХ ГОСПОДАРЮЮЧИХ СУБ'ЄКТІВ В СУЧАСНИХ УМОВАХ ЗА СИСТЕМАТИЗОВАНОГО УПРАВЛІННЯ РИЗИКАМИ

Капелюшна Т. В., к. е. н., доц., Голобородько С.О.
Державний університет телекомунікацій
м. Київ, Україна

Останні декілька років світ стикається з новими викликами, які діють іззовні і на які підприємства, що функціонують в умовах невизначеності, не можуть впливати. Саме тому господарюючим суб'єктам потрібно адаптуватися під до цих змін та формувати відповідні до вимог часу та умов: підходи до управління безпекою підприємства, методи оцінки, критерії оцінки безпеки, враховувати нові фактори впливу на безпеку підприємств. Лише за вчасного реагування на зовнішні виклики можна досягти безпеки у функціонуванні, створювати сприятливі умови з огинанням небезпек, що потенційно можуть виникнути.

Система управління безпекою підприємства в невизначених умовах, які наразі на собі відчувають всі господарюючі суб'єкти, організації, держава та суспільство має трансформуватися, з урахуванням загроз, ризиків, що викликані сьогоднішніми умовами. Інакше – система зазнає руйнівних змін, які призведуть до деструктивних змін на мікрорівні, а згодом – макрорівні.

Процес управління є складним і потребує деталізації при побудові системи управління безпекою з урахуванням усіх складових безпеки, об'єктів захисту та суб'єктів безпеки, інструментів, що можливі для застосування, поглибленим вивченням факторів впливу та оточення, методів управління безпекою з

розмежуванням викликів, загроз та ризиків, які потенційно можливі, або ж наявні з подальшими методами оцінки для побудови ефективної системи управління ризиками підприємства.

Управління безпекою підприємств являє собою процес оцінки ризиків безпеки, з подальшим планування заходів щодо їх усунення, спрямованих на подолання викликів, що пов'язані з роботою в небезпечному, складному несприятливому середовищі, нині - в невизначеному.

У нинішніх умовах ризик можна визначити як ймовірність зіткнення із загрозою та потенційними наслідками зіткнення із загрозою [1].

Доцільним є створення спільних рамок для визначення ризиків, що загрожують підприємствам в окремих сферах з попередньо проведеним їх ранжуванням, щоб чітко визначитися з найбільш загрозливими, та виокремленням пріоритетних із них з подальшою розробкою плану стримування або ж прийняття, у разі неможливості його усунення. У свою чергу, таке виокремлення дозволить ранжовані ризики відносити до різних категорій та таких, які неможливо усунути, з метою оптимізації та економії часу для упередження їх дії за пріоритетністю.

Нині умови вимагають надшвидкої реакції на критичні інциденти небезпеки на підприємствах та миттєвого управління кризовими ситуаціями. За наявності плану антикризового планування при управлінні безпекою та завчасного його використання вдасться усунути виявлені ризики.

Враховуючи сьогоденні загрози, підприємства повинні переорієнтовуватися та використовувати підходи до управління ризиками та стійкістю безпеки, щоб упереджувати дію невизначених умов на функціонуючі підприємства. Так як, дія зовнішніх ризиків надсильна, а вплив на них з боку функціонуючих підприємств може бути мінімальним, виникає потреба у спільній побудові структури визначення та оцінки ризиків не лишень підприємствами, але й урядами, зовнішніми стейкхолдерами, тоді можна розраховувати на довгострокову ефективну та безпечну роботу підприємств та організацій. Варто будувати систему управління ризиками, починаючи із визначення ризиків, з якими може зіткнутися підприємство з виділенням найбільш характерних для певної галузі (як партерну) та категорізації ризиків, спираючись на їх ознаки (товарні ризики, ринкові, і т.д.). Після чого потрібно обрати потенційні методи їх зниження, впровадити та протестувати методи їх усунення з подальшим оцінюванням придатності методів усунення (прийняття або відхилення), і останнє – контроль ефективності визначених категорійованих ризиків та застосовуваних методів їх зниження щодо доцільності використання з плином часу.

Систематизоване управління ризиками з використанням розроблених рамок визначення ризиків з їх ранжуванням за ступенем дестабілізації показників ефективності роботи підприємства, що функціонує в конкретній сфері, допоможе вчасно прийняти рішення про те, які із заходів є доцільними для забезпечення безпеки досліджуваного підприємства в сучасних умовах.

Література:

1. Кравченко М.О., Бояринова К.О., Копішинська К.О. (2021). *Управління ризиками.* Навчальний наочний посібник. Київ : КПІ ім. Ігоря Сікорського, 2021. 432 с.

СЕКЦІЯ 3. ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Ніколабай А.О.
Державний університет телекомунікацій
м. Київ, Україна

У зв’язку з загальним розповсюдженням комп’ютерних технологій все більш актуальною є проблема захисту інформації. Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними випадками порушення безпеки інформації можна вважати несанкціонований доступ - доступ до інформації, що здійснюється з порушенням установлених правил [1].

Одним із ключових елементів захисту від несанкціонованого доступу до будь-якої інформаційної комп’ютерної системи є ефективна система ідентифікації. У загальному випадку ідентифікація об'єкта – це його упізнання, ототожнення із ким-небудь (чим-небудь). Цей процес необхідний для того, щоб система надалі змогла ухвалити рішення щодо видачі людині дозволу для роботи на комп'ютері, доступу до закритої інформації тощо. Таким чином, ідентифікація є одним із основних понять в інформаційній безпеці [2].

Сьогодні існують три методи ідентифікації: парольна, апаратна та біометрична. Головним недоліком парольного та апаратного методів, які засновані на використанні карток, електронних ключів, а також паролів і кодів доступу, є неоднозначність ідентифікованої особистості. Цей недолік можна усунути, використовуючи біометричні методи ідентифікації. Біометрична ідентифікація – це спосіб визначення особи за окремими специфічними біометричними ознаками, властивими конкретній людині.

Головною перевагою біометричних технологій є найвища надійність і точність, оскільки перевіряються параметри, які дуже важко або неможливо змінити або підробити. Ідентифікація користувачів за біометричними характеристиками може розглядатися як альтернатива парольній системі або її доповнення. Використання будь-якого паролю чи пристрою разом із біометричною ідентифікацією дає можливість створити найкращий захист інформаційних систем [3].

Існує безліч методів біометричної ідентифікації, які можна розділити на дві великі групи: статистичні та динамічні. Статистичні методи ґрунтуються на фізіологічній характеристиці людини, яка дана її від народження: ДНК, відбитки пальців, райдужна оболонка ока. Динамічні методи спрямовані на перевірку характеристик, набутих особою з часом: почерк, голос або хода.

Кожен біометричний метод має свої переваги і недоліки. Крім цього, різні біометричні методи ідентифікації дуже сильно залежать від мети призначення і сфери застосування. Поки що тільки три біометричні методи довели свою масову практичність: розпізнавання за відбитками пальців, райдужною оболонкою очей та рисами обличчя (2D і 3D-методи) [4].

Технологіями біометричної ідентифікації користуються сотні мільйонів людей в різних країнах світу. Якщо в 2001 році обсяг біометричного ринку в світі становив усього 300 млн доларів, то вже в 2006 році він зріс до 2 млрд доларів, а в 2018 року становив $17,28 млрд. Такі дані наводять аналітики ResearchAndMarkets. При цьому експерти стверджують, що світовий ринок обладнання та програмного забезпечення для біометрії знаходиться на підйомі і залишиться таким і надалі. Очікується, що витрати на такі продукти збільшуватимуться приблизно на 18% щорічно і досягнуть $17,28 млрд до 2027 року. Такі показники свідчать про те, що значення біометричних технологій у комплексному забезпеченні безпеки постійно зростає [5].

Отже, вже сьогодні в багатьох країнах існують десятки тисяч комп'ютеризованих місць, сховищ, дослідницьких лабораторій, банків крові, банкоматів, військових споруд, доступ до яких контролюється пристроями, що базуються на використанні біометричних технологій. В Україні також спостерігаються тенденції впровадження новітніх систем: перехід до біометричних паспортів як засобів ідентифікації особи, використання біометричних методів перевірки особи під час банківських операцій. Максимальну ефективність захисту банківських операцій здатні забезпечити такі системи, в яких поєднуються декілька різних видів біометричної ідентифікації, або ж комбіновані види автентифікації, зокрема, апаратні (наприклад, електронні ключі) та біометричні технології.

Література

1. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

2. Попиріна О.О. Поняття про ідентифікацію. URL: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-identifikaciu

3. Царьов Р.Ю., Лемеха Т.М. Біометричні технології : Навчальний посібник. Одеса : ОНАЗ ім. О. С. Попова, 2016. 140 с.

4. Бідюк П., Бондарчук В. Сучасні методи біометричної ідентифікації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. 2009. Вип. 1(18). С. 137-146.

5. Захаров В.П., Рудешко В.І. Біометричні технології в XXI столітті та їх використання правоохоронними органами : Посібник. Львів: ЛьвДУВС, 2015. 492 с.

АУДИТ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

Нечай А.І.
Державний університет телекомунікацій
м. Київ, Україна

Контроль є складовою управління суспільним відтворенням. Будь-яке суспільство не може нормально функціонувати і розвиватися без чітко організованої системи контролю за виробництвом і розподілом суспільного продукту та іншими сферами суспільного життя. Контроль являє собою діяльність, спрямовану на попередження, фіксацію й усунення порушень та недоліків у різних сферах суспільного життя. Поняття контроль є багатогранним, відображає різні аспекти його реалізації. Глибшому усвідомленню самого поняття «контроль» сприяє його поділ на окремі види, тобто класифікація контролю. Залежно від організаційних форм розрізняють державний, відомчий, внутрішньогосподарський та аудиторський контроль.

Аудиторський контроль здійснюють незалежні особи (аудитори), аудиторські фірми, які уповноважені суб'єктами господарювання. Він може здійснюватися з ініціативи суб'єктів господарювання, а також у випадках, передбачених чинним законодавством. Залежно від форми проведення та системи контрольних дій розрізняють перевірку, ревізію та аудит. Перевірка являє собою обстеження і вивчення окремих ділянок фінансово-господарської діяльності товариства, установи або їхніх підрозділів. Наслідки перевірки оформляються довідкою або доповідною запискою.

Ревізія – це форма документального контролю за фінансово-господарською діяльністю товариства, установи, дотриманням законодавства з фінансових питань, достовірності обліку й звітності, спосіб документального викриття недостач, розтрат, привласнень та крадіжок коштів і матеріальних цінностей, попередження фінансових зловживань. За наслідками ревізії складається акт.

Аудит, відповідно до Закону України «Про аудиторську діяльність», – це перевірка публічної бухгалтерської звітності, обліку, первинних документів та іншої інформації щодо стану фінансово-господарської діяльності суб'єктів господарювання з метою визначення достовірності їх звітності, обліку, його повноти і відповідності чинному законодавству та встановленим нормативам.

Аудит поділяється на зовнішній і внутрішній. Зовнішній аудит проводиться незалежним (зовнішнім) аудитором (аудиторською фірмою) для визначення стану банку на основі аналізу обліку і звітності, а також має на меті підтвердження (непідтвердження) фінансової звітності банку. Згідно з положеннями Закону України «Про Національний банк України» Рада Національного банку не пізніше 1 листопада звітного року приймає рішення про аудит НБУ і визначає аудиторську фірму, яка має відповідний досвід роботи, для перевірки річного звіту і подання аудиторського висновку. Національний банк зобов'язаний відповідно до укладеного з аудиторською фірмою договору

надавати звітність та інформацію, необхідну для проведення аудиторської перевірки.

Внутрішній аудит – це незалежна діяльність аудиторської служби банку з перевірки й оцінки діяльності центрального апарату та структурних підрозділів банку в його інтересах. Внутрішні аудитори здійснюють більш глибокий (ніж зовнішні аудитори) аналіз, перевірку, оцінку та вивчення різних аспектів банківської діяльності. Це пов'язано з функціями, які притаманні внутрішньому аудиту. Основні завдання внутрішнього аудиту в банках полягають у такому:

1. забезпечення відповідної схоронності банківських активів, документів, майна та цінностей;
2. перевірка та оцінка адекватності та ефективності системи внутрішнього банківського контролю;
3. проведення ідентифікації та управління банківськими ризиками;
4. перевірка дотримання структурними підрозділами банку чинного законодавства та нормативно-правових актів НБУ у процесі здійснення банківських операцій;
5. перевірка повноти й достовірності даних бухгалтерського обліку й звітності, відповідності правил їх ведення і складання чинному законодавству;
6. розроблення пропозицій щодо усунення виявлених недоліків і порушень та запобігання їх у подальшому;
7. оцінювання нинішніх дій банку з погляду досягнення стратегічних цілей і завдань у майбутньому;
8. надання працівникам функціональних підрозділів банку консультацій з різноманітних питань, пов'язаних з банківською діяльністю.

Він поєднує у собі прийоми і методи фактичного і документального контролю, що дає змогу найбільш повно і змістовно перевірити операції банку, ефективність використання ресурсів, які перебувають у розпорядженні банку. Особливості аудиту у банках обумовлені специфікою документального та облікового оформлення операцій, а також розвинутою системою внутрішньобанківського контролю.

Ефективність аудиту значною мірою залежить не лише від якості його здійснення, а й від організації контролю за виконанням рішень, прийнятих за висновками аудиту. У практичній роботі НБУ застосовуються різні способи контролю за виконанням ухвалених за висновками аудиту рішень: одержання письмових звітів про виконання пропозицій та рекомендацій за висновками аудиту; перевірка виконання рішень, ухвалених за висновками аудиту, за даними звітності та іншими матеріалами, що надходять від структурних підрозділів, які аудитувалися; перевірка на місці, яка здійснюється працівниками служби аудиту; перевірка прийнятих рішень у ході наступного аудиту структурного підрозділу.

Література
1. Розпорядження 05.06.2014 № 1772 Про затвердження Порядку проведення внутрішнього аудиту (контролю) у фінансових установах URL: https://zakon.rada.gov.ua/laws/show/z0885-14#Text
2. Закон України Про аудит фінансової звітності та аудиторську діяльність URL: https://zakon.rada.gov.ua/laws/show/2258-19#Text

ФІШИНГ ЯК ПОСЛУГА

Запорожченко М.М.
Державний університет телекомунікацій
м. Київ, Україна

Фішинг як послуга (Phishing-as-a-Service, PhaaS) – це різновид організованої кіберзлочинності, при якому кіберзлочиці через Інтернет пропонують іншим послуги фішингу в обмін на гроші. Фішинг – це різновид шахрайства, при якому в більшості випадків в якості методу комунікації використовується електронна пошта, через яку кіберзлочиці відправляють повідомлення потенційними жертвами, при цьому маскуючись під законну компанію чи особу для того, щоб обманом змусити жертву або розкрити свої конфіденційні дані, наприклад, логіни, паролі, номери рахунків користувачів банківських сервісів, платіжних систем, соціальних мереж, поштових сервісів, різноманітних провайдерів тощо, або ж завантажити на свій пристрій шкідливе програмне забезпечення для подальшого розгортання атаки. Отримані від жертв дані можуть бути використані для фінансового шахрайства, крадіжки особистих даних, для доступу до облікових записів жертв, шантажу, продажу в дарквебі [1].

Провайдери PhaaS продають доступ до інструментів та послуг, необхідних для здійснення фішингової атаки. Якщо раніше для розгортання результативної фішингової кампанії зловмисник повинен був володіти широким набором знань та вмінь, то з появою фішингу як послуги навіть новачок здатен вдало здійснити подібну атаку. Якщо раніше реклама подібних сервісів проводилася виключно в даркнеті, то наразі можна знайти пропозиції і у відкритому доступі. Якщо пропозиція зацікавила клієнта, він може придбати набір для фішингу, який містить все необхідне для проведення фішингової атаки, наприклад, шаблони електронних листів, які відправляються жертвам, шаблони сайтів-підробок, у деяких випадках навіть список потенційних цілей, детальні інструкції та підтримку клієнтів. Тобто можна сказати, що всі ці набори призначені для тих людей, які хочуть брати участь у кібератаках, але не мають технічних навичок для того, щоб зробити це самостійно.

Так, наприклад, аналітиками компанії Mandiant було виявлено PhaaS-сервіс під назвою «Caffeine» [2], який дозволяє будь-якому зловмиснику проводити власні фішингові компанії завдяки відкритому процесу реєстрації та відсутності необхідності отримання користувачами схвалення адміністратора. В більшості

подібних послуг використовуються система підписок, і Caffeine не є виключенням. В залежності від тривалості підписки та функцій пропонуються 3 тарифи (рис. 1), проте варто зазначити, що ця ціна перевищує середню вартість підписки на PhaaS приблизно у 3-5 разів, оскільки Caffeine пропонує системи антивиявлення та антианалізу, а також послуги підтримки клієнтів.

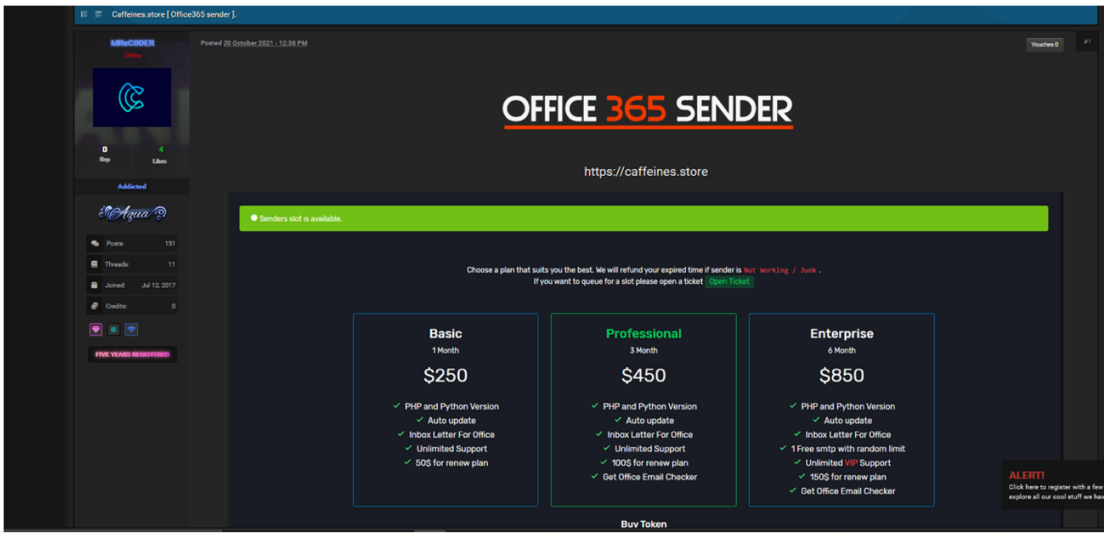


Рис. 1. Вартість тарифів Caffeine

Проблемою також є те, що подібні платформи з ростом їх популярності будуть приваблювати все більше хакерів, які, власне, створюють набори та інструменти для фішингових кампаній, оскільки вони ускладнюють їх переслідування. Так, хакер може розробити набір інструментів для фішингу, при цьому не здійснивши жодної атаки. І навіть якщо користувач, якому цей набір для фішингу буде продано, буде спійманий органами влади, сам розробник набору може уникнути судового переслідування та продовжувати продавати свій продукт і отримувати прибуток.

Висновки. Перед звичайною фішинговою атакою вразливі як окремі особи, так і організації, а її успішне проведення може призвести як до злому особистих облікових записів, так і до проникнення кіберзлочинця в корпоративні мережі. Для успішної реалізації подібних атак зловмисник повинен володіти широким набором знань та навичок, однак з появою фішингу як послуги ця умова вже не є обов'язковою, оскільки доступність та розвиток PhaaS дозволяють будь-якій особі, незалежно від рівня її кваліфікації, здійснювати такі атаки, що ще більше підкреслює необхідність та актуальність захисту від фішингових атак.

Література

1. Andreea Chebac. What Is Phishing-as-a-Service (PhaaS)? 2022. URL: https://heimdalsecurity.com/blog/what-is-phishing-as-a-service-phaas/

2. Adrian McCabe, Steve Sedotto. The Fresh Phish Market: Behind the Scenes of the Caffeine Phishing-as-a-Service Platform. 2022. URL: https://www.mandiant.com/resources/blog/caffeine-phishing-service-platform

МЕТОДИЧНИЙ ПІДХІД ДО ЗАБЕЗПЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ Й ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТУ

Якименко Ю.М., Д'ячук О.С.
Державний університет телекомунікацій,
м. Київ, Україна

Ключовим поняттям в управлінні безперервністю бізнесу виступає «інцидент», під яким розуміється будь-яка незапланована, раптова подія, подія, що веде до зупинки ключових, критичних процесів і функцій, повній втраті контролю над устаткуванням.

Інциденти інформаційної безпеки (ІБ) можуть впливати безпосередньо чи опосередковано на бізнес-діяльність організації. Недостатня підготовка конкретної організації до виявлення і обробки таких інцидентів збільшує ступінь негативного впливу на бізнес. У більшості організацій є матеріальні ресурси, інтелектуальна власність, комп'ютери, комунікаційні канали, будинки. Якщо хоча б щось одне із цього переліку буде ушкоджене або недоступне по тій або іншій причині, організації може бути нанесений збиток або виникнути надзвичайна ситуація, після яких може статися катастрофа і порушення бізнесу.

Таким чином, для будь-якої організації, що серйозно ставиться до ІБ, важливо застосовувати структурний і плановий підхід до:

- виявлення, оповіщення про інциденти ІБ і їх оцінці;
- витягу уроків з інцидентів інформаційної безпеки, уведенню превентивних захисних заходів і поліпшенню загального підходу до менеджменту інцидентів ІБ;
- реагування на інциденти ІБ, включаючи активізацію відповідних захисних заходів для запобігання, зменшення наслідків і (або) відновлення після негативних впливів і, в першу чергу, в областях підтримки й планування забезпечення безперервності бізнесу [1].

Тема доступності, цілісності й конфіденційності по відношенню до інформаційних ресурсів проходить центральною ланкою в забезпеченні безперервності бізнесу [1].

Засоби управління доступом повинні завжди захищати цілісність і/або конфіденційність інформаційного ресурсу. Фактично, засіб управління доступом повинне виконувати безліч кроків для неможливості несанкціонованої зміни його вмісту в процесі використання.

Цілісність і конфіденційність інформаційних ресурсів повинні забезпечуватися не тільки при виконанні повсякденних процедур, але й при виконанні процедур у випадку виникнення інциденту ІБ.

Також, важливо відзначити, що організація при виникненні аварії або надзвичайної ситуації може стати значно більш уразливою, оскільки використовувані для її захисту сервіси безпеки можуть виявитися недоступні або працювати з обмеженими можливостями. Тому для організації, яка має безліч

різних секретів, дуже важливо забезпечити конфіденційність і цілісність даних і систем навіть у випадку, якщо співробіники й сама організація перебувають у складному становищі. В цьому разі доступність розглядається як один з основних аспектів планування безперервності бізнесу і потрібно забезпечити гарантії постійної доступності до критичних ресурсів організації. Для цього може знадобитися належне виконання резервного копіювання, забезпечення надмірності в архітектурі систем, мереж і виконуваної діяльності. На випадок неприступності комунікаційних каналів протягом тривалого періоду часу, повинен існувати швидкий і перевірений спосіб створення альтернативних комунікацій і пов'язаних з ними сервісів. Для управління безперервністю бізнесу, щоб допомогти організаціям мінімізувати ризик виникнення збоїв, був розроблений стандарт ISO 22301. Почавшись із банального резервного копіювання інформації, система управління безперервністю бізнесу поступово охопила крім питань ІБ практично всі аспекти ділової активності, перетворившись у цілісну структуру поглядів на методи забезпечення безперервності бізнесу – стійкості організації до всіляких збоїв, руйнувань і втратам [3]. Вимоги стандарту носять універсальний характер і можуть бути застосовані будь-якою організацією, незалежно від типу, розміру або виду діяльності.

Планування безперервності бізнесу організації повинно:

- забезпечити негайну й правильну реакцію в надзвичайній ситуації;
- захистити життя людей і гарантувати їхню безпеку;
- мінімізувати негативний вплив на бізнес організації;
- відновити виконання критичних для бізнесу функцій;
- скористатися послугами зовнішніх постачальників на період відновлення
- знизити безладдя й плутанину під час кризи;
- забезпечити виживання бізнесу компанії;
- забезпечити максимально швидке відновлення функціонування після аварії.

Хоча немає чіткого підходу щодо планування безперервності бізнесу, але час від часу з'являються різні кращі практики на цей рахунок. Зокрема, NIST (NISTonal Institute of Standards and Technology, США), який відповідає за розробку кращих практик і забезпечення загального доступу до них, передбачив наступні **кроки підходу** до **планування безперервності бізнесу для ІТ-систем** в документі [2]:

1. ***Розробити політику планування безперервності бізнесу*** (continuity planning policy statement). Написати політику, яка буде містити необхідні керівні принципи для розробки плану **BCP** (business continuity plan – план забезпечення безперервності бізнесу) і визначить необхідні ролі повноваження для виконання покладених на них завдань.

2. ***Провести Аналіз впливу на бізнес*** (**BIA**–business impact analysis). Ідентифікувати критичні функції й системи, категоризувати (пріоритезувати) їх

на основі ступеня їх критичності. Виявити уразливості й загрози, розрахувати ризики.

3. ***Визначити превентивні захисні заходи***. Після виявлення загроз, вибрати і впровадити захисні заходи й контролі для зниження рівня ризиків компанії економічно доцільним способом.

4. ***Розробити стратегії відновлення*** (recovery strategy). Описати методи, що забезпечують оперативне відновлення працездатності критичних систем і функцій.

5. ***Розробити план дій на випадок надзвичайних ситуацій*** (contingency plan).Описати процедури, розробити керівництва, які забезпечать продовження функціонування компанії в аварійному стані.

6. ***Протестувати план, провести тренінги й навчання***. Перевірити план для виявлення недоліків у ньому, провести тренінги й навчання для належної підготовки людей до виконання завдань на випадок надзвичайної ситуації.

7. ***Підтримувати актуальність плану***. Ужити заходів для своєчасної актуалізації плану.

У деяких компаніях на практиці передбачаються підходи, аналогічні зазначеним, але з іншою термінологією. Безперервність бізнесу є фундаментальною частиною програми загальної безпеки організації, тому дуже важливо переконатися в їхній відповідності один до одного.

Література

1. Безперервність бізнесу та відновлення після нещасних випадків.Частини 1 і 2. Домен ISSP 07.URL: http://dorlov.blogspot.com/2010/10/issp-07-1.html.
URL: http://dorlov.blogspot.com/2010/10/issp-07-2.html.
2. SP 800-34 « Посібник із планування безперервності для IT-Систем». URL: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf/.
3. ISO 22301: 2012 Системи управління безперервності бізнесу.

ФОРМУВАННЯ ОБІЗНАНОСТІ ПЕРОНАЛУ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Урсатій Я. О.
Державний університет телекомунікацій
Київ, Україна

Розвиток глобального процесу інформатизації суспільства, що спостерігається в останні десятиліття, спричинив нову глобальну проблему – забезпечення безпеки інформації. Багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства.

Не випадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом все більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі. Тому обізнаність персоналу є важливим елементом забезпечення інформаційної безпеки організації. Оскільки багато атак на інформаційні системи здійснюються через дії або недбалість персоналу, необхідно забезпечити правильну інформаційну освіту, щоб персонал міг розуміти потенційні ризики та вмів адекватно реагувати на них.

Одним з основних елементів програми формування обізнаності є навчання персоналу основам безпеки інформації, яке повинно включати ознайомлення з найбільш поширеними видами кібератак, методами захисту від них, правилами безпеки при обробці даних та користування комп'ютерами та іншими електронними пристроями. Дослідження, проведені компаніями щодо ефективності інформаційних та навчальних заходів [1] підтверджують, що регулярне проведення інформаційних кампаній та тренінгів із питань захисту інформації для персоналу компанії сприяє зниженню кількості інцидентів інформаційної безпеки, зокрема пов’язаних із використанням методів соціальної інженерії.

Дослідженнями науковців встановлено, що в умовах цифровізації діяльність організацій і підприємств із формування обізнаності грунтується на програмних продуктах, навчання персоналу постійно репрезентує нові вирішення, які забезпечують досягнення цілей інформаційної безпеки кожного підприємства. Новітні програмні розроблення фокусуються на формуванні безпечної поведінки та корпоративної культури безпеки, залучають користувачів до альтернативних методів (гейміфікації, мікронавчання та віртуальної реальності), пропонують позитивний, надійний і легкий для сприйняття зміст,

надають замовнику всебічну і неперервну підтримку незалежно від його локалізації [2].

Варто проводити регулярні атестації, які допоможуть виявити слабкі місця в системі захисту і внести необхідні зміни для підвищення рівня безпеки.

Категорії працівників, які підлягають атестації, та періодичність її проведення визначаються колективним договором. На підприємствах, в установах та організаціях, у яких не укладаються колективні договори, категорії працівників, які підлягають атестації, строки та графік її проведення визначаються роботодавцем за погодженням з виборним органом первинної профспілкової організації [3].

Атестація працівників проводиться не частіше ніж один раз на три роки. Вона організовується рішенням роботодавця, яким затверджуються положення про проведення атестації, склад атестаційної комісії, графік проведення атестації. Інформація про проведення атестації доводиться до відома працівників не пізніше ніж за два місяці до її проведення.

У процесі формування обізнаності персоналу необхідно також забезпечити мотивацію співробітників для виконання правил та процедур інформаційної безпеки. Це може бути досягнуто за допомогою різноманітних заохочень, включаючи бонуси, премії та можливість просування по кар'єрній драбині [4].

Загалом, формування обізнаності персоналу є важливим інструментом забезпечення інформаційної безпеки в організації. Це можна реалізувати за допомогою використання різноманітних методів навчання персоналу, а також створення культури безпеки в організації.

Література

1. IT best of breed. *IT Best of Breed*. URL: http://i.crn.com. (дата звернення: 18.02.2023).

2. Про професійний розвиток працівників : Закон України від 12.01.2012 р. № 4312-VI : станом на 27 груд. 2019 р. URL: https://zakon.rada.gov.ua/laws/show/4312-17#Text (дата звернення: 30.03.2023). (дата звернення – 19.02.2023).

3. Мужанова Т. М. Засоби інформування й навчання персоналу у сфері інформаційної безпеки в умовах цифровізації. *Зв'язок* 2021. Т. 152 № 4, С. 14-16. URL: DOI: 10.31673/2412-9070.2021.041416. (дата звернення – 18.02.2023).

4. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві. *Економіка пром-сті.* 2010. № 3. С. 123-129. URL: http://dspace.nbuv.gov.ua/handle/123456789/24811 (дата звернення – 19.02.2023).

МЕТОДИ ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Щавінський Ю.В., к.т.н., Жеребило В.О.
Державний Університет Телекомунікацій
Київ, Україна

Високі темпи розвитку інформаційно-комп'ютерних технологій, стрімка модернізація сервісів обміну інформацією породили нові непередбачувані можливості для маніпуляції інформацією. Доступність інформації створює загрози її втрати або несанкціонованої передачі з метою отримання вигоди. Особливу потенціальну небезпеку для організацій і підприємств складають інсайдери, які володію інформацією з внутрішніх першоджерел. Вони можуть краще оцінити стан справ, ніж будь-який інший фахівець, який користується зовнішньою інформацією для експертного висновку. Тому проблема інсайдерських загроз втрати даних потребує особливої уваги керівників при плануванні заходів інформаційної безпеки [1].

Окремі проблемні питання протидії інсайдерським загрозам розглядали у своїх працях вітчизняні дослідники А. С. Бевза, Г.М.Гулак, Б. А. Кормич, І. П. Мігус, І. М. Мужик, Т. В. Німченко, В. С. Цимбалюк, С. Ф. Філоненко [2-5].
Як зазначать науковці, проблема витоку інформації стає все більш актуальною у всіх сферах людської діяльності. Різні сфери діяльності мають різну вразливість до інсайдерських загроз і ступінь вразливості залежить від характеру діяльності організацій. Тому організації застосовують різні методи і особливі підходи до управління такими загрозами.

Оскільки інсайдери мають доступ до цінних інформаційних ресурсів, недоступних для сторонніх осіб, збитки, спричинені атаками інсайдерів, можуть бути руйнівними. Крім того, ці загрози зростають за масштабами, масштабами та витонченістю; таким чином, наголошуючи на критичній необхідності організацій застосовувати сучасні методи безпеки. Для виявлення вторгнень застосовують моніторинг мережі. Для більш ефективних дій організації формують політику прогнозування інсайдерських атак, яка визначає і регулює дії та поведінку персоналу в організації. Ця політика закріплюється у корпоративних кодексах, положення яких обов'язкові до виконання усіма членами організації. Планують заходи спрямовані на виявлення і реагування на внутрішні загрози, якщо атака відбувається або уже відбулась. За допомогою моніторингу, записів у журналі, інформаторів.

В роботі [6] запропонована модель передбачення інсайдерських загроз, яка складається із двох частин: перша – аналіз нетипової поведінки в інформаційних системах в режимі реального часу на основі зібраної інформації системи виявлення вторгнень та системних сигналів; друга – аналіз такого компоненту, як психологічне профілювання. Це дозволяє передбачити потенційну загрозу інсайдерів, виявивши зв'язок між психологічною складовою і технічними параметрами системи захисту для прогнозування схильності до зловмисної.

Таким чином, методи виявлення інсайдерських загроз є складним інструментом інформаційної безпеки підприємств і організації, що потребує комплексного підходу до врахування особливостей діяльності та врахування психологічних особливостей працівників при створенні системи захисту.

Література

1. Лисенко С. О. Інсайдерські загрози інформаційній безпеці у виконавчому провадженні. *Право.ua*. 2020. № 2. С. 48–53. URL: https://doi.org/10.32782/law.2020.2.7 (дата звернення: 30.03.2023).
2. Бевза А. С. Правове забезпечення інформаційної безпеки ринку цінних паперів в Україні : дис. … канд. юрид. наук : 12.00.07. Київ, 2020. 242 с.
3. Гулак Г. М. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. *Сучасний захист інформації*. 2017. Т. 2, № 30. С. 65–71.
4. Мігус І. П. Розголошення інсайдерської інформації як загроза економічній безпеці акціонерних товариств. *Інвестиції: практика та досвід*. 2012. № 3. С. 20–23.
5. Філоненко С. Ф. Система попередження витоку персональних даних мережевими каналами. *Ukrainian scientific jornal of information security*. 2014. Т. 20, № 3. С. 279–285.
6. Заікін С. Ф. Модель передбачення інсайдерської загрози в організації. *Сучасний захист інформації*. 2021. Т. 1, № 45. С. 30–34.

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Герасимов А.О.
Державний університет телекомунікацій
м. Київ, Україна

На сьогоднішній день своєчасна та об’єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників. Проте глобальна комп’ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави.

«Оцінка ефективності програми навчання з питань безпеки на підприємстві». Досліджується ефективність програми навчання з питань безпеки на підприємстві. Дослідження оцінює вплив програми на поведінку співробітників і їх здатність розпізнавати загрози безпеці та реагувати на них. Результати показують, що комплексна та постійна програма навчання може

значно знизити ризик людської помилки, яка є основною причиною порушень безпеки.

«Оцінка ефективності систем управління інформаційною безпекою на підприємстві». Це дослідження оцінює ефективність систем управління інформаційною безпекою (СУІБ) на підприємстві. Дослідження оцінює впровадження та підтримку СУІБ, включаючи оцінку ризиків, розробку політики, контроль безпеки та аудит. Результати свідчать про те, що структура СУІБ є ефективним підходом до управління ризиками інформаційної безпеки та може допомогти організаціям захистити свої активи та репутацію [1].

«Вимірювання ефективності контролю доступу на підприємстві». У цьому документі розглядається ефективність контролю доступу в корпоративному середовищі. Дослідження оцінює дизайн, впровадження та моніторинг засобів контролю доступу, включаючи механізми автентифікації, авторизації та звітності. Результати показують, що добре розроблені та керовані засоби контролю доступу можуть значно знизити ризик несанкціонованого доступу та витоку даних.

«Оцінка ефективності рішень із захисту кінцевих точок на підприємстві». Це дослідження оцінює ефективність рішень для захисту кінцевих точок у корпоративному середовищі. Дослідження оцінює впровадження та управління рішеннями безпеки кінцевих точок, включаючи антивірусне програмне забезпечення, брандмауери та системи виявлення вторгнень. Результати свідчать про те, що комбінація рішень для захисту кінцевих точок може забезпечити ефективний захист від зловмисного програмного забезпечення, мережевих атак та інших загроз безпеці.

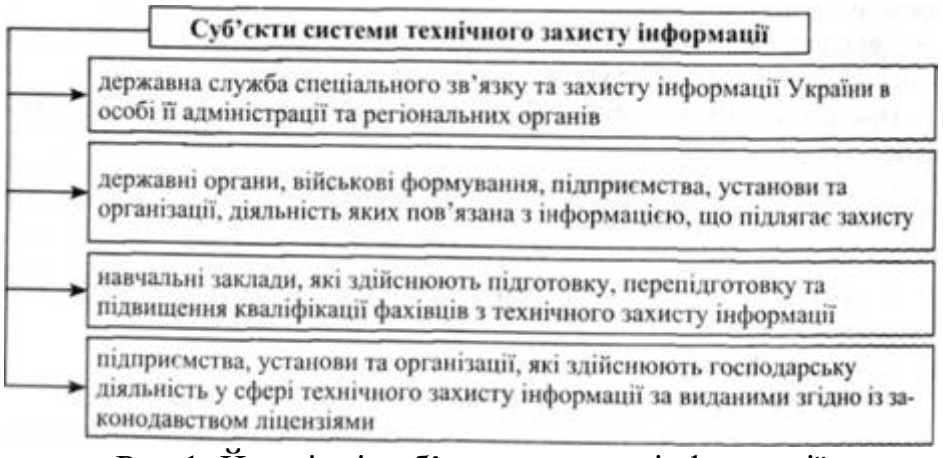


Рис.1. Ймовірні суб'єкти захисту інформації

Ефективність засобів і методів захисту інформації на підприємстві можна оцінити за допомогою різних методик, таких як:

Оцінка ризику: комплексна оцінка ризику може допомогти виявити потенційні вразливі місця та загрози для інформаційних систем підприємства. Ця оцінка повинна охоплювати як внутрішні, так і зовнішні загрози, включаючи фізичні, технологічні та людські загрози.

Тестування на проникнення. Тестування на проникнення передбачає імітацію атаки на інформаційні системи підприємства для виявлення слабких місць, якими можуть скористатися зловмисники. Цей тест може допомогти оцінити ефективність заходів безпеки підприємства та визначити сфери, які потребують покращення [2].

Аудити безпеки. Аудити безпеки включають незалежну оцінку засобів контролю та процесів безпеки підприємства. Ці перевірки можуть проводитися внутрішніми або зовнішніми аудиторами та можуть надати уявлення про ефективність заходів безпеки підприємства.

Оцінки відповідності: оцінки відповідності оцінюють відповідність підприємства відповідним нормативним вимогам і галузевим стандартам. Ця оцінка може допомогти переконатися, що підприємство дотримується найкращих практик і відповідає вимогам законодавства щодо інформаційної безпеки.

Тестування реагування на інциденти: Тестування реагування на інциденти передбачає імітацію інциденту безпеки для оцінки процедур реагування підприємства. Цей тест може допомогти виявити прогалини в плані реагування на інциденти підприємства та покращити здатність організації реагувати на інциденти безпеки.

У висновку, ефективна оцінка засобів і методів захисту інформації підприємства має бути всебічним і безперервним процесом, який передбачає комбінацію методів, згаданих вище. Ця оцінка може допомогти переконатися, що інформаційні активи підприємства захищені від потенційних загроз і вразливостей.

Література

1. Організація і функції підрозділів технічного захисту інформації URL:https://pidru4niki.com/1374072251330/ekonomika/organizatsiya_funktsiyi_pidrozdiliv_tehnichnogo_zahistu_informatsiyi
2. Міністерство внутрішніх справ україни національна академія внутрішніх справ Рибальский О.В., хахановський В.Г., Кудінов В.А. Організація і функції підрозділів технічного захисту інформації URL: https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ОБЛАСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Дворниченко В.О., Недодай М.Г.
Державний університет телекомунікацій
м. Київ, Україна

Захист інформаційного простору стає все більш актуальною темою в сучасному світі. Існує безліч шляхів, за допомогою яких зловмисники можуть

отримати доступ до конфіденційної інформації, включаючи соціальну інженерію.

Соціальна інженерія - це методика, що використовує людські фактори для отримання несанкціонованого доступу до конфіденційної інформації, підману або інші зловживання. Це може стати серйозною загрозою для інформаційного простору які містять конфіденційну інформацію, особисті дані та інші цінності.

Сучасні дослідження підтверджують важливість захисту інформаційного простору від соціальної інженерії, наприклад:

- "State of the Phish 2020" від компанії Proofpoint - 96% всіх атак відбуваються через людей, а також більше 88% організацій зазнали атаки фішингу протягом 2020 року.
- Verizon Data Breach Investigations Report за 2021 рік - соціальна інженерія була застосована у більш ніж 20% випадків кібератак, зокрема відправка фішингових листів, які намагаються переконати людину надати свої особисті дані або іншу конфіденційну інформацію. Також зазначається, що атаки з використанням соціальної інженерії стали більш розповсюдженими під час пандемії COVID-19, коли збільшилась кількість працівників, які перейшли на дистанційну роботу.
- KnowBe4 за 2020 рік - найбільш поширеною технікою соціальної інженерії є фішингові листи, які становлять більш ніж 90% усіх інцидентів, пов'язаних з соціальною інженерією. Крім того, дослідження показало, що більше 40% людей натискатимуть на посилання в фішингових листах, якщо вони виглядають достатньо вірогідними.
- IBM X-Force Threat Intelligence Index за 2021 рік - соціальна інженерія є найбільш популярним методом атак на користувачів, оскільки вона дозволяє зловмисникам впливати на поведінку своєї жертви, а не просто зламати систему або використати шкідливе програмне забезпечення.

Методи захисту інформаційного простору від соціальної інженерії:

Один з найбільш ефективних методів захисту від соціальної інженерії- це навчання користувачів. Користувачі повинні розуміти які загроз можуть стати на шляху безпеки їхньої інформації, та знати, як реагувати на них. Навчання повинне включати розуміння того, що таке фішинг, смішинг, соціальний інженеринг по телефону та інші види атак, які використовують вразливості людської психології. Крім того, користувачі повинні бути навчені розпізнавати підозрілу активність та як поводитися в такій ситуації.

Застосування двофакторної автентифікації може стати важливим методом захисту від соціальної інженерії. Це означає, що для доступу до інформації потрібно буде ввести два коди, наприклад, пароль і код підтвердження, який надсилається на мобільний телефон користувача.

Шифрування даних може допомогти захистити конфіденційну інформацію від несанкціонованого доступу. Шифрування можна застосовувати для захисту даних, що передаються по мережі, а також для зберігання даних на пристроях.

Використання програмних засобів для захисту інформаційного простору може бути дуже корисним. Наприклад, антивіруси, брандмауери та інші

програмні засоби можуть допомогти забезпечити захист від зловмисного програмного забезпечення та інших атак.

Для компаній можна додати наступні методи:

Розроблення політик безпеки, що визначають процедури захисту інформації, такі як паролі, обмеження доступу та інші, може допомогти забезпечити безпеку інформаційного простору від соціальної інженерії.

Моніторинг може допомогти виявити спроби соціальної інженерії та забезпечити реагування на них. Інструменти моніторингу можуть включати перегляд логів, аналіз мережевої активності та використання різних програмних засобів для виявлення зловмисних дій.

Література

1. 10 ways businesses can prevent social engineering attacks - hitachi systems security. *Systèmes de Sécurité Hitachi*. URL: https://hitachi-systems-security.com/10-ways-businesses-can-prevent-social-engineering-attacks/.
2. 10 ways businesses can prevent social engineering attacks | indusface blog. *Indusface*. URL: https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/.
3. Ethical hacking: Social engineering basics | Infosec Resources. *Infosec Resources*. URL: https://resources.infosecinstitute.com/topic/ethical-hacking-social-engineering-basics/.

СЕКЦІЯ 4. ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ

ПАРАМЕТРИЧНИЙ МЕТОД СПЕКТРАЛЬНОГО АНАЛІЗУ РАДІОСИГНАЛІВ

Собчук А.В., PhD, Лаптєв С.О. аспірант
Державний університет телекомунікацій
м. Київ Україна

Останнім часом зріс інтерес до параметричних методів спектрального аналізую. Методи спектрального аналізу випадкових сигналів діляться на два великі класи — непараметричні і параметричні. У непараметричних методах використовується тільки інформація, що міститься у даних аналізованого сигналу. Параметричні методи передбачають наявність деякої статистичної моделі випадкового сигналу, а процес спектрального аналізу в даному випадку містити визначення параметрів цієї моделі.

Значна роль в аналізі сигналів належить комплексному перетворенню Фур'є. Перетворення Фур'є (ПФ) і його дискретні аналоги (ДПФ) добре відомі та широко застосовуються в техніці спектрального аналізу при стандартній обробці радіосигналів. Воно ефективно в обчислювальному відношенні та просто в реалізації. Як правило, такі процедури дають хороші результати при аналізі частотного складу тривалих за часом радіосигналів. Однак відомі причини, що обмежують застосування перетворення Фур'є при аналізі коротких сигналів, якими можуть бути цифрові радіоімпульси наприклад, використання ДПФ для усічених за часом сигналів призводить нас до ефектів Гіббса, які спотворюють інформацію про спектр сигналу і не дають можливості забезпечити високу точність в спектральної області при аналізі гармонійних компонент.

Використання віконного перетворення Фур'є покращує оцінювання спектрів, але не дає повного розв'язання зазначеної проблеми.

Виконані за останні кілька десятиліть всебічні дослідження з питань цифрового спектрального оцінювання привели до істотного розвитку сучасних технологій в цій галузі. Прагнення до знаходження перетворень, які краще відповідають невеликої тривалості сигналів, що володіють довільним тимчасово-просторовим становищем, призвело до появи вейвлет-аналізу. В його основі лежать короткі функції, що володіють тимчасової (просторової) і частотною локалізацією, що дає кращу апроксимацію для коротких сигналів і дозволяє точніше визначати їх гармонійні компоненти. Однак використання вейвлет-аналізу при обробці радіосигналів може мати деякі обмеження з точки зору інтерпретації, що пов'язано з формальним вибором деяких ортогональних функцій як базису відповідного перетворення. З вищевикладеного можна зробити висновок що питання перетворення радіо сигналів з подальшим його аналізом остаточно не вирішене і вимагає постійного вдосконалення.

Одним з методів, що дозволяють вирішити вказані недоліки є параметричний метод спектрального аналізу Проні, що використовує уявлення спостережуваного процесу у вигляді комплексного експоненціального ряду. Метод дозволяє за відліком сигналу знайти параметри цих комплексних експонент, що, у свою чергу, дає можливість записати вираз для спектральної щільності досліджуваного сигналу. Широке застосування методу Проні стало можливим тільки останнім часом, оскільки він істотно нелінійний і вимагає великих обчислювальних витрат. У зв'язку з цим виникла необхідність детального дослідження даного методу з точки зору оптимальності його математичної реалізації, а також потенційної стійкості до флуктуацій відліків сигналу і шумів дискретизації.

Нами розглянуто методи спектрального аналізу засновані на використанні будь-якої моделі для опису сигналу, тобто при їх використанні робляться деякі припущення про поведінку сигналу поза інтервалу спостереження. Завдання спектрального оцінювання при цьому зводиться до знаходження параметрів використовуваної моделі, яка вибирається виходячи з наявної апріорної інформації про досліджуваний процес. Запропоновано метод спектрального аналізу, на основі класичного метода Проні, який удосконалений шляхом заміни загасаючих синусоїд на використання незгасних синусоїд, що дозволяє дуже точно виділити сигнал і визначити його характеристики на тлі дуже багатого на перешкоди ефірного простору. Застосовано алгоритм швидкого перетворення для вирішення нормальних рівнянь знаходження змінних для послідовного визначення параметрів сигналу таких як амплітуда, частота та фаза.

Висновки: Огляд методів спектрального аналізу показав, що метод спектрального аналізу, на основі класичного метода Проні, який удосконалений шляхом заміни загасаючих синусоїд на використання незгасних синусоїд, дозволяє дуже точно виділити сигнал і визначити його характеристики на тлі дуже багатого на перешкоди ефірного простору. З метою підтвердження обраного методу спектрального аналізу, проведено моделювання та отримані графіки спектрограм імпульсного сигналу за допомогою методів Фур'є, Чебішева, Бесселя. Отримані графічні дані цілком підтверджують переваги запропонованого нами метода, для спектрального аналізу випадкових короткочасних імпульсів.

Література

1. Improving the method of searching digital illegal means obtaining information based on cluster analysis / O. Laptiev et al. *Scientific journal of astana IT university*. 2020. No. 3. P. 63–70. URL: https://doi.org/10.37943/aitu.2020.99.72.006 (date of access: 30.03.2023).

2. Методика вибору оптимального вхідного сигналу радіомоніторингу для програмних засобів на базі перетворення фур’є / A. Musienko та ін. *Системи управління, навігації та зв’язку. Збірник наукових праць*. 2019. Т. 4, № 56. С. 135–140. URL: https://doi.org/10.26906/sunz.2019.4.135

ТИПОВА АРХІТЕКТУРА SECURITY OPERATION CENTER В КОМПАНІЇ

Довірак М. І.
Державний університет телекомунікацій,
Київ. Україна

Ландшафт безпеки різко змінився за останні кілька років, і зараз з кожним роком організації мають справу з складнішими кібератаками. Кіберзлочинці постійно знаходять нові способи обійти системи безпеки, викрасти дані та зламати системи. У відповідь компанії інвестують у центри безпеки (SOC), щоб захистити свої системи та дані. Операційні центри безпеки стали ефективним підходом до кібербезпеки, що дозволяє компаніям контролювати свої системи, виявляти загрози та реагувати на них, а також проактивно керувати ризиками безпеки. SOC складається з кількох технологій і продуктів, які разом забезпечують комплексну інфраструктуру безпеки [1].

Архітектура SOC включає різні технології, які працюють узгоджено для захисту активів компанії. Наприклад, система безпеки та управління подіями (SIEM) збирає й аналізує дані з різних джерел, таких як брандмауери, системи виявлення вторгнень і антивірусне програмне забезпечення, щоб виявити підозрілу поведінку або моделі, які можуть вказувати на кібератаку. Система виявлення та реагування на кінцеві точки (EDR) проактивно відстежує кінцеві пристрої, такі як ноутбуки, настільні комп'ютери, сервери, тонки клієнти та навіть IoT, на наявність будь-якої підозрілої активності, запобігаючи втраті або крадіжці даних

На додаток до технологій, які використовуються в архітектурі SOC, для створення надійної інфраструктури безпеки необхідні кілька продуктів. Фаерволи наприклад, є першою лінією захисту в інфраструктурі безпеки компанії. Вони блокують несанкціонований доступ до мережі та запобігають проникненню зловмисного трафіку в мережу. Системи виявлення та запобігання вторгненням (IDPS) відстежують мережевий трафік і виявляють будь-яку підозрілу поведінку чи шаблони. Антивірусне програмне забезпечення захищає кінцеві пристрої від зловмисного та іншого шкідливого програмного забезпечення. Система SIEM також може надавати сповіщення в реальному часі про потенційні загрози, дозволяючи аналітикам безпеки реагувати швидко та ефективно. Ця можливість особливо важлива в сучасному динамічному середовищі загроз, де зловмисники можуть швидко переміщатися по мережах, що ускладнює виявлення загроз і реагування на них [2].

Система EDR також може надати цінну інформацію про поведінку користувачів, наприклад про незвичайні входи або незвичайні шаблони доступу до файлів. Цю інформацію можна використовувати для виявлення потенційних внутрішніх загроз і запобігання втраті даних.

Третьою технологією, що використовується в архітектурі SOC, є система аналізу мережевого трафіку (NTA) або сучасніший підхід по виявленню та

реагуванні на мережеві інциденти (NDR). Система NTA/NDR призначена для моніторингу мережевого трафіку та аналізу його на наявність ненормальної поведінки. Система може виявляти постійні загрози, які не можуть бути виявлені традиційними системами безпеки, і реагувати на них. Система NTA має вирішальне значення для захисту активів компанії, оскільки вона надає інформацію про мережеву діяльність, виявляючи потенційні вразливості та загрози. Система NTA/NDR також може надати цінну інформацію про продуктивність мережі та допомогти виявити потенційні проблеми продуктивності мережі, які можуть вплинути на доступність і продуктивність системи.

Таким чином, ми можемо зробити висновок, що стандартна та типова архітектура SOC складається з системи управління подіями інформаційної безпеки (SIEM), управління та захист кінцевих точок (EDR), виявлення та реагування на мережеві аномалії (NDR). В більшості організацій, саме вони є основними інструментами операційної команди безпеки та зарекомендували себе як ефективний метод для забезпечення кібернетичної безпеки в організації [4].

Література

1. Gathner – How to Build and Operate Security Operation Center. URL: https://www.gartner.com/en/documents/4002259
2. SANS – Building and Leadning Security Operation Center. URL: https://www.sans.org/cyber-security-courses/building-and-leading-security-operations-centers/
3. SANS 2021 Survey – Security Operation Center (SOC). URL: https://assets.extrahop.com/whitepapers/sans-2021-soc-survey.pdf
4. A design model for SOC. URL: https://www.deitauditor.nl/informatiebeveiliging/a-design-model-for-a-security-operations-centre-soc/

ПРОГРАМНІ ЗАСОБИ МОНІТОРИНГУ Й УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Шевченко Д.К.
Державний університет телекомунікацій
м. Київ, Україна

Сучасні інформаційні технології повністю інтегровані в усі сфери людської діяльності. Інтернет об'єднує не лише комп'ютери та смартфони окремих користувачів, але й корпоративні мережі. Компанії 24 години на добу обмінюються інформацією та документами між відділами, постачальниками, партнерами та клієнтами через свої внутрішні мережі з метою підвищення операційної ефективності. З розвитком технологій зростає і рівень загроз для

використання інформаційних технологій. Мережі та служби передачі даних піддаються ризику масштабних атак з боку зловмисників: вже більше десяти років злочинці активно здійснюють різні злочини і злочинну діяльність у сфері інформаційних технологій. У відповідь на нові атаки розробляються нові або вдосконалюються старі методи захисту інформації та інформаційно-технологічної інфраструктури компаній.

На сьогоднішній день інформаційна безпека компаній та організацій піддається численним загрозам. Серед загроз, з якими стикаються компанії, - зовнішні вторгнення в мережу компанії, що призводять до недоступності сервісів компанії, крадіжки конфіденційних даних та інформації, втрати контролю над веб-трафіком, проникнення вірусів і так званих "троянських коней", а також різні види внутрішніх і зовнішніх загроз для компанії та її діяльності.

Для забезпечення захисту необхідна система моніторингу інформаційної безпеки підприємства. Це SIEM-система, що допомагає організаціям виявляти, аналізувати й усувати кіберзагрози, перш ніж вони зможуть нашкодити бізнес-процесам. SIEM поєднує в одному рішенні інструменти управління інформаційною безпекою та управління подіями безпеки. Це дозволяє краще керувати системами безпеки Технологія SIEM збирає дані журналу подій з різних джерел і використовує аналіз в режимі реального часу для виявлення нетипових дій і вжиття відповідних заходів [1].

Коротше кажучи, SIEM покращує видимість подій у всій корпоративній мережі, дозволяючи організаціям швидко реагувати на потенційні кібератаки і підтримувати відповідність нормативним вимогам. За останнє десятиліття технологія SIEM розвинулася до використання штучного інтелекту для більш швидкого та ефективного виявлення та реагування на загрози [1].

Правильний підбір інструментів SIEM залежить від потреб організації. Залежно від вимог, компанії можуть обирати інструменти відповідно до їхніх можливостей щодо дотримання нормативних вимог та виявлення загроз.

Нижче наведені деякі з найкращих інструментів управління інформацією про безпеку та подіями, доступних на ринку [2]:

1. Менеджер подій SolarWinds Security Гарний інтерфейс з великою кількістю візуалізації графічних даних виступає перед потужним і всебічним інструментом SIEM, який працює на Windows Server.
2. ManageEngine EventLog Analyzer Інструмент SIEM, який керує, захищає та мінує файли журналу. Ця система встановлюється в Windows, Windows Server та Linux.
3. Splunk Enterprise Security Цей інструмент для Windows та Linux є світовим лідером, оскільки поєднує мережевий аналіз та управління журналами разом із відмінним інструментом аналізу.
4. OSSEC Система безпеки HIDS з відкритим кодом, яка вільна у використанні та діє як служба управління інформацією про безпеку.
5. LogRhythm Security Intelligence Platform Найсучасніша технологія на основі AI лежить в основі цього інструменту аналізу трафіку та журналів для Windows та Linux.

6. Уніфіковане управління безпекою AlienVault Велике значення SIEM, яке працює на Mac OS, а також Windows.

7. RSA NetWitness Надзвичайно всебічний та пристосований до великих організацій, але трохи надто для малих та середніх підприємств. Працює в Windows.

8. IBM QRadar Провідний на ринку інструмент SIEM, який працює в середовищах Windows.

9. Менеджер безпеки McAfee Enterprise Популярний інструмент SIEM, який працює через записи Active Directory для підтвердження безпеки системи. Працює на Mac OS, а також Windows.

Таким чином, інформаційна безпека в сучасних підприємствах вважається одним з найважливіших елементів комплексної безпеки, незалежно від рівня - держави, галузі, компанії або приватної особи. Для забезпечення оптимального рівня захисту необхідна система моніторингу інформаційної безпеки підприємства. Це SIEM-система, спрямована на моніторинг ключових подій та інцидентів інформаційної безпеки, які відбуваються в компанії та її діяльності.

Література

1. Що таке SIEM? | Захисний комплекс Microsoft URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem

2. 9 кращих інструментів SIEM: Посібник з інформації про безпеку та управління подіями URL: https://instagalleryapp.com/chistij-administrator-2/9-krashhih-instrumentiv-siem-posibnik-z-informacii

МЕТОДИ ВИЯВЛЕННЯ ШАХРАЙСЬКОЇ ІНТЕРНЕТ-РЕКЛАМИ ПРИ ОРГАНІЗАЦІЇ БЕЗПЕКИ ІНТЕРНЕТУ

Папуча Н.В
Державний університет телекомунікацій
м. Київ, Україна

В епоху інформаційних технологій сучасний бізнес не може розвиватися без реклами в інтернеті. Найбільша концентрація реклами розміщується переважно популярних веб-сайтах, що добре себе зарекомендували: Google, на новинних сайтах, на сайтах про технології, у соціальних мережах, у застосунках на телефоні, у відео в ютубі і так далі.

Інтернет-реклама адресована масовому клієнту і має характер переконання. Вона дозволяє вирішувати практично всі завдання, що стоять перед комерційним web-сайтом, будь це Інтернет-магазин, сервісні послуги або дистриб'ютори.

Сьогодні Інтернет-реклама також стає більш доступною для і малого бізнесу. Переважна більшість компаній вже давно почали перерозподіляти свій бюджет на користь реклами в Інтернеті, поступово скорочуючи обсяги

традиційних видів просування, оскільки вони вже не настільки ефективно виконують свої функції.

Поряд із великими перевагами інтернет-реклами завдяки використанню інформаційних технологій за сприяння держави забезпеченню доступності та сумісності електронних комунікаційних послуг [1], використання реклами в інтернеті має і свої недоліки у вигляді дорвей-сайтів (веб-сторінок з безглуздим але «релевантним» вмістом, що перенаправляє відвідувачів на інший сайт) для просування інших сайтів за допомогою посилань, псевдо-сайтів (сайтів-підробок, фальшивих сайтів фірм або клубів, фальшивих Інтернет-магазинів, фан-клубів і т. д.) для шахрайства, присвоюючи гроші користувачів собі.

Основними ознаками псевдо-сайтів є: мінімум інформативних сторінок; відсутність назви (у шапці дублюється адреса); відсутність контактної інформації (як контакти представлена тільки форма зворотного зв'язку або e-mail на безкоштовному ящику). Для боротьби із шахрайством інтернет-реклами створюються організації, які залучають фахівців кібербезпеки, кампанії виділяють кошти для розробки методів боротьби із шахрайством.

Одним із розроблених методів є використання фільтрації захисними системами одним із найбільших постачальників інтернет-послуг GOOGLE [2. Цей метод включає дві підситеми [3]. Перша підсистема проводить онлайн-фільтрацію. На цьому етапі всі характеристики трафіку аналізуються в режимі реального часу, визначаються як суто статистичні аномалії (кліки із переліку заблокованих IP-адрес), так і більш складні, наприклад, наявність відомих шаблонів нападу. Друга підсистема працює в режимі оффлайн та аналізує трафік, враховуючи його передісторію. На цьому етапі виділяються більш складні атаки. Також будь-який рекламодавець може особисто надіслати запит в службу підтримки компанії Google. Такі запити розглядаються людьми, які підтверджують або заперечують наявність шахрайства. У випадку позитивної відповіді компанія зобов’язується повернути кошти за недійсні кліки (покази). Дані про шахрайську поведінку на рекламних сайтах зберігаються у базі даних. На етапі детального аналізу система намагається відшукати в даних трафіку вже відомі шаблони шахрайської поведінки. Якщо такі були знайдені, генерується відповідний сигнал для рекламодавця [4].

Але, не зважаючи на існуючі методи захисту від шахрайської інтернет-реклами, чорними хакерами розробляються та застосовуються нові способи шахрайства, що потребує також розроблення нових методів боротьби з ними, створення відповідних органів та підготовки фахівців.

Література

1. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX : станом на 1 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 09.02.2023).

2. Chertov O., Malchykov V., Pavlov D. Non-Dyadic wavelets for detection of some click-fraud attacks. *International conference on signals and electronic systems, ICSES* : International Conference, Gliwice, 7 September 2023. Gliwice, 2010. P. 401–404.
3. How google detects invalid clicks - A must know for adsense publisher. *SG & Singapore Map! Powered by Streetdirectory.com*. URL: https://www.streetdirectory.com/etoday/-euajfw.html.
4. Павлов Д. Г. Захист рекламної інтернет-кампанії від мережевого шахрайства. *Наукові праці Чорноморського державного університету імені Петра Могили* : наук. журн. Миколаїв, 2012. Т. 191. С. 81–86.

ЗАСТОСУВАННЯ НЕЙРОНИХ МЕРЕЖ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Тішков М.С.
Державний університет телекомунікацій
м.Київ, Україна

Із зростанням рівня цифровізації у всіх галузях, зростає попит на забезпечення належним рівнем безпеки важливих для підприємств даних та компонентів інформаційних систем. Кожен інструмент захисту інформації має на меті швидке та точне виявлення шкідливого програмного забезпечення, яке має на меті зашкодити підприємству. Одним з прогресивних методів у галузі створення інструментів безпеки є використання нейронних мереж.

Більшість інструментів захисту інформації покладаються на конкретні індикатори та шаблони для виявлення загрози. Зазвичай вони розпізнають лише ті загрози, про які їм уже відомо і не ефективні проти невідомих загроз.

Алгоритми із використанням нейронних мереж, можуть підлаштовуватися під властивості даних, на яких вони навчаються. Це полегшує автоматичну адаптацію до величезної кількості загроз. У той час як звичайні алгоритми вимагають занадто багато людського втручання. Нейронна мережа у процесі використання продовжує розвиватися та з часом навчається завчасно розпізнавати загрози, з якими раніше не зустрічалася, і запобігати їх дії.

Основні засоби захисту інформації, які потребують використання нейронних мереж та вже їх використовують – це [1] :

- Системи антивірусного захисту
- Системи виявлення та запобігання вторгненням (IDS/IPS)
- Системи попередження втрати даних (DLP)
- Системи управління інформаційною безпекою та подіями (SIEM)
- Анти-DDOS системи

Для тих чи інших системи захисту інформації можуть для кращої дієздатності використовуватися різні моделі нейронних мереж але при

коректному використанні точність виявлення цільових шкідливих об’єктів досягає 99% [2].

Можливі застосування нейронних мереж для забезпечення захисту приватної інформації підприємств, які є основними для забезпечення високого рівня реалізації інформаційної безпеки [3]:

- процес навчання дозволяє привести найточніший ступінь розпізнавання даних на вході та підвищити стійкість мережі до завад. Дана властивість необхідна для точної оцінки візуального образу (різних знаків, указників та розпізнавання лиць);

- застосування деяких властивостей нейронних мереж та підвищення кількості шарів нейронів дозволяє підвищити точність оцінки вхідних даних та збільшити можливість виявлення помилок, які будуть втрачені за роботи звичайних систем без інтелектуального аналізу;

- безперервний аналіз процесу обробки даних під час роботи дозволить виявити непомітні раніше зв’язки, які можна використовувати для коректування роботи самої системи у цілому, що дозволить підвищити загальну ступінь захисту мережі підприємства;

- результати роботи штучних нейронних мереж виражаються ймовірністю виникнення даної події, тобто система з такою основою дозволяє зіставляти закономірності вірусних атак та отримувати ймовірності їх появи. Зі збільшенням часу роботи, мережа накопичують досвід, що дозволяє робити припущення про виникнення нападів і можливості їх запобігання;

- швидкість роботи системи зі застосуванням нейронних мереж значно вища ніж звичайної системи без інтелектуального аналізу. Це дозволяє за менших затратах обчислюваної потужності, швидше виявляти, знешкоджувати та реагувати на атаки.

Сучасні засоби захисту інформації, які використовують шаблонний аналіз не мають можливості виявлення нових загроз, а також потребують більше часу для підтримки їх бази знань. Саме тому використання нейронних мереж дозволить виявляти нові загрозити та підвищити показники ефективності виявлення вже існуючих загроз.

Література

1. Exploring the Application of Deep Learning in Cyber Security By Stuart Rauch URL: https://www.simplilearn.com/application-of-deep-learning-in-cyber-security-article

2. Recurrent neural networks for Cyber security use-cases By Mohammed Harun Babu R, Vinayakumar R, Soman KP
URL: https://arxiv.org/ftp/arxiv/papers/1901/1901.04281.pdf

3. Use of Neural Networks for Predicting Cyberattacks By Bohdan Bebeshko, Karyna Khorolska, Nataliia Kotenko, Oleksander Kharchenko, Tetyana Zhyrova URL: https://ceur-ws.org/Vol-2923/paper23.pdf

РОЗРОБЛЕННЯ КОМПЛЕКСНОГО МЕТОДУ ВИЯВЛЕННЯ НАЙБІЛЬШ ВПЛИВОВИХ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ В СУЧАСНИХ УМОВАХ.

Базарний С.В.
Національний університет оборони України
м. Київ, Україна

За останні кілька років соціальні мережі значно змінили наш спосіб спілкування та обміну інформацією. Нині вони стали потужним інструментом впливу на громадську думку та поведінку людей. Серед безлічі користувачів соціальних мереж існують особи, які мають значний вплив на інших, вони можуть стати відправною точкою інформаційної хвилі, викликати масштабні рухи або впливати на формування думок та переконань. Тому виявлення найбільш впливових користувачів соціальних мереж стало дуже важливою задачею для різних галузей, включаючи політику, дослідження громадської думки, військової сфери де їх розуміння та використання є важливим інструментом.

Проблема полягає в тому, що в соціальних мережах існує велика кількість користувачів, серед яких деякі мають значно більший вплив на інших. Метод виявлення таких ключових гравців є важливим для розуміння та аналізу соціальних мереж, що дозволить виявляти та використовувати їх вплив для досягнення конкретних цілей. Одним з викликів є визначення критеріїв, за якими користувачі можуть бути визнані впливовими. Крім того, існує необхідність у розробці ефективних алгоритмів для виявлення таких користувачів, особливо у великих мережах з великою кількістю взаємодій. Дослідження впливових користувачів соціальних мереж можуть мати важливе значення для бізнесу, маркетингу, політики та інших галузей. Декілька зарубіжних вчених, які займаються розробкою методів ідентифікації ролей та впливу користувачів на соціальні мережі, визначення рівня їх впливу, а також програмного забезпечення для їхньої автоматизації для підтримки прийняття рішень при протидії цілеспрямованим деструктивним впливам:

Jure Leskovec, професор на кафедрі електротехніки та комп'ютерних наук у Стенфордському університеті, який спеціалізується на аналізі соціальних та інформаційних мереж. Він брав участь у розробці методів виявлення впливових користувачів та ролей в соціальних мережах;

Lada Adamic, професор на кафедрі інформаційних наук у Мічиганському університеті, яка займається дослідженнями соціальних мереж, включаючи розробку методів виявлення впливових користувачів та їх ролей у мережах. Проте, в цій області активно працюють й інші дослідники з університетів та наукових центрів США, Канади, Великобританії, Німеччини, Італії та інших країн. Серед них можна виділити таких вчених, як Maksym Gabielkov, Kiran Garimella, Emilio Ferrara, Kristina Lerman, Huan Liu, та інших.

Однак, не всі з цих методів і програм мають ідеальну точність та ефективність у виявленні ролей користувачів та їхнього впливу на соціальні мережі. Наприклад, деякі методи можуть працювати лише з обмеженою кількістю соціальних мереж, або не давати достатньо точних результатів у випадку складних мереж зі значною кількістю взаємодій між користувачами. Також, багато з програмного забезпечення мають обмеження у розмірі мережі, яку вони можуть обробити за раз, що може затримати аналіз у разі великих мереж.

Наприклад, Жозефіна Горн та її колеги з Університету Оксфорда розробили метод для виявлення впливових користувачів на Twitter, що базується на аналізі залежності між розміром аудиторії користувачів та їх впливом на мережу. Однак, цей метод не дозволяє виявляти ролі користувачів в інших соціальних мережах та може давати неточні результати у випадку, коли користувачі мають низький рівень активності на мережі. Отже, хоча багато вчених займаються розробкою методів та програмного забезпечення для виявлення ролей та впливу користувачів на соціальних мережах, важливо зрозуміти, що жоден з цих методів не є універсальним та не має ідеальної точності. Деякі з цих авторів також пропонують практичні рішення для вирішення проблем, пов'язаних зі соціальними мережами. Наприклад, Sinan Aral пропонує розробку нових методів для зменшення впливу фейкових новин на політичні процеси, а Zeynep Tufekci досліджує, як можна підвищити стійкість мережевих протестів до різних видів атак.

У той же час, інші автори, такі як Duncan Watts та Filippo Menczer, звертають увагу на те, що підходи, які можуть вважатися очевидними і правильними, насправді можуть бути невірними. Вони намагаються з'ясувати, як ми можемо зрозуміти, чому ми ухвалюємо ті чи інші рішення, і з якими обмеженнями ми стикаємося в цьому процесі. Інші автори, такі як David Easley та Jon Kleinberg, пропонують широкий огляд різних аспектів мережевої науки, включаючи теоретичні та практичні аспекти аналізу мережевих структур. В цілому, ці автори допомагають зрозуміти різноманітні виклики, які виникають в сучасному світі соціальних мереж, та пропонують різні інструменти та підходи для їх вирішення. До найпопулярніших сучасних соціальних мереж належать наступні:

Facebook - за даними компанії Statista, у 2021 році число щомісячних активних користувачів Facebook складає 2,91 млрд осіб по всьому світу.

YouTube - за даними компанії Google, на кінець 2020 року сервіс YouTube має 2,3 млрд зареєстрованих користувачів та більше 1 млрд годин відео, переглянутих кожного дня.

WhatsApp - за даними компанії Statista, на кінець 2020 року популярний месенджер WhatsApp має більше 2 млрд активних користувачів щомісяця.

Instagram - за даними компанії Hootsuite, на кінець 2021 року Instagram має понад 1,3 млрд активних користувачів щомісяця.

TikTok - за даними компанії SensorTower, на кінець 2020 року TikTok має понад 1,1 млрд активних користувачів щомісяця.

Для визначення найвпливовіших користувачів соціальних мереж можна використовувати різні методи, залежно від того, яка мета аналізу. Одним з підходів є аналіз мережі зв'язків між користувачами, який називається "аналіз соціальних мереж". Нижче наведено деякі методи, які можуть допомогти визначити найвпливовіших користувачів соціальних мереж.

Центральність - це міра того, наскільки центральним є користувач у мережі. Центральність може бути обчислена за допомогою різних метрик, таких як ступінь виходу (кількість зв'язків, які має користувач), ступінь входу (кількість зв'язків, які спрямовані на користувача), близькість (як далеко користувач від інших у мережі), та інші.

Впливовість - це міра того, як великий вплив має користувач на інших у мережі. Це може бути обчислено за допомогою різних метрик, таких як PageRank, HITS, та інші.

Кластеризація - це процес групування користувачів за спільними ознаками, такими як інтереси, місцезнаходження, або інші. Кластеризація може допомогти визначити найвпливовіших користувачів в кожній групі.

Взаємодія - це міра того, наскільки часто взаємодіють користувачі між собою. Взаємодія може бути обчислена за допомогою різних метрик, таких як кількість лайків, коментарів, повідомлень, які отримує користувач, та інші.

Найбільший деструктивний вплив через соціальні мережі здійснюють користувачі, які мають максимальний рівень інформаційного впливу. Існуючі методики, що використовуються для їх ідентифікації, не враховують деякі суттєві характеристики, у тому числі ролі найвпливовіших користувачів (НВП), через що експертам доводиться обробляти велику кількість профілів і витрачати багато часу на ідентифікацію користувачів, що підлягають моніторингу чи впливу. Таким чином, для підтримки прийняття рішень при протидії цілеспрямованим деструктивним впливам на соціальні мережі актуальним науковим завданням є розробка ефективних методів ідентифікації ролей користувачів та рівня їх впливу на соціальну мережу, а також програмного забезпечення для їхньої автоматизації.

Література

1. Прібилєв Ю. Б., Базарний С. В. Спосіб визначення місцезнаходження користувачів соціальних мереж. *Забезпечення кібероборони держави* : Зб. матеріалів III науково-практ. вебінару, м. Київ. Київ, 2022. С. 160–162.
2. Facebook MAU worldwide 2022 | statista. *Statista*. URL: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.
3. WhatsApp: number of monthly active users 2020 | Statista. *Statista*. URL: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/.
4. YouTube revenue and usage statistics (2023). *Business of Apps*. URL: https://www.businessofapps.com/data/youtube-statistics/.

ДОСЛІДЖЕННЯ IP-ПРОТОКОЛІВ ДЛЯ КОМП'ЮТЕРНИХ МЕРЕЖ ЗА КРИТЕРІЯМИ БЕЗПЕКИ

Хомяков Р.В.
Державний університет телекомунікацій
м. Київ, Україна

IP (Internet protocol) – є невід'ємною частиною всесвітньої мережі. Саме за допомогою нього, величезна кількість локальних мереж набула можливості комунікувати між собою без урахування різних канальних технологій. Однак, на жаль, з новими технологіями приходить велика відповідальність, а разом з ним і проблеми вже іншого масштабу. Так ,недоліки IP протоколів змусили створити різні протоколи безпеки, транспортний рівень і вище, які забезпечують не тільки комфортне користування інтернетом, а й гарантію цілісності передачі вашої інформації.

Почнемо з того, що являє собою мережевий рівень і які основні відмінності між канальним рівнем..Мережевий рівень – надає можливість маршрутизації та надсиланням даних між різними мережами. Основними і найважливішими протоколами на цьому рівні є IP та ICMP. Наразі, використовують дві основні версії IP протоколу:IPv4, IPv6.

IP (Internet protocol) – інтернет протокол, що містить набор правил для маршрутизації та адресації пакетів, за допомогою яких, пакет має можливість переміщатися та досягати пункту призначення. Кожний пакет містить в собі інформацію про IP,де вказані адреси відправника та одержувача. Таким чином, роботу IP можна порівняти з надсилання листа по почті, де на листі в у строго визначеному порядку вказано ім'я, вулиця, місто та поштовий індекс. Основні технологія мережевого та канального рівня Ethernet,WIFI - не підходять для створення WAN, оскільки їх таблиці комутації можуть обробляти лише певну кількість хостів, на відміну від глобальної мережі, де існує мільярд хостів.

IPv4 – четверта версія IP, яка працює за принципом обміну пакетами. Він може лише ідентифікувати пристрої, підключені до мережі через систему адресації. IPv4 має 32-бітну довжину адреси, дозволяючи зберігати приблизно 4,19 млрд. адрес.

Головною особливістю цього протоколу є призначення кожному пристрою унікальну адресу. В цьому і полягає головна проблема,32 бітний адресний простір, що використовується IPv4 обмежує кількість пристроїв. Саме тому на вирішення цієї проблеми був створений протокол NAT та 6 версія IP протоколу. Найбільш помітною відмінністю від версії 4 є розмір адрес, IPv4 використовує 32 біти для адресації, а IPv6 використовує 128-бітові адреси, що забезпечують с.3,4 × 10 38 адрес. Незважаючи на багато переваг IPv6 над 4 версією, сфера застосування IPv4 більша, ніж IPv6. Це відбувається внаслідок низки проблем, таких як проблемне розгортання, погана сумісність з існуючою інфраструктурою. Саме це призведе до уповільнення переходу на більш

досконалу версію. На даний момент більшість трафіку все ще проходиться на IPv4, тоді як тільки 30-35% використовують нову версію IP протоколу.

Мережева інфраструктура вважається вже сама по собі ненадійною за, в будь-якому середовищі передачі, бо не існує центрального моніторингу, який би слідкував за станом мережі. Щоб не навантажувати мережу, всі складні функції були перекинуті на кінцевий вузол. На момент створення IP протоколів, мова не йшла про забезпечення безпеки та цілісності. Основним його завданням є надання можливості маршрутизації між різними мережами. IP є ненадійним протоколом, оскільки він не гарантує доставку дейтаграми до місця призначення. Надійність доставки пакету забезпечується протоколами верхнього рівня, такими як TCP. Ось тому, можна виділити основі недоліки мережевого протоколу з точки зо безпеки:

- IP не слідкує за потоком та не забезпечує повторну передачу;
- Відсутність механізмів шифрування;
- Не гарантує правильну та надійну доставку пакету.

Проблему з доставкою пакетів вирішує TCP протокол. Також, він гарантує порядок доставки, в якому вони були надіслані. Однією з важливих умов забезпечення безпечної передачі даних є протоколи безпеки, яким і є IPsec, який виправляє більшість недоліків IP протоколу.

IPSec — набір певних протоколів, які забезпечують безпеку та цілісність пакетів під час передачі в мережі. IPSec став життєздатним стандартом мережевої безпеки, оскільки підприємства хотіли забезпечити безпечну передачу даних через Інтернет. IPSEC забезпечує такі послуги:

- Визначення алгоритмів і ключів для створення захищеного з'єднання;

- Шифрування пакетів. Пакети, якими обмінюються дві сторони, можуть бути зашифровані за допомогою одного з алгоритмів шифрування та спільного ключа;

- Цілісність даних, гарантія того, що пакет не змінюється під час передачі. Якщо отриманий пакет не проходить перевірку цілісності даних, він відхиляється;

Підсумовуючи, можна точно переконається в тому, що сам по собі IP протоколи розглядати з погляду безпеки неправильно. Протоколи мережного рівня дають можливість передачу даних у глобальній мережі їх не захищаючи і гарантуючи цілісність доставки. За критеріями безпеки IP протоколи не мають механізмів аутентифікації, шифрування, контроль за потоком даних, що відправляються. Все вищеописане забезпечується протоколами безпеки такими як IPsec або протоколом транспортного рівня TCP.

Література

1. TCP/IP Illustrated, Volume 1: The Protocols" by W. Richard Stevens - This book provides a detailed overview of the TCP/IP protocol suite, including the IP protocol and its security features.

2. Kaur, N., & Singh, D. (2021). Security challenges and solutions in Internet of Things: A review. Journal of Ambient Intelligence and Humanized Computing, 12(1), 725-750.
3. Al-Turjman, F., Awwad, A., & Khalil, I. (2021). A Review of Internet of Things Security Challenges and Proposed Solutions. IEEE Internet of Things Journal, 8(2), 811-828.
4. Kim, S., & Kim, S. (2021). A survey on security threats and countermeasures in the software-defined networking environment. Journal of Communications and Networks, 23(1), 46-60.

ПРОЦЕСНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮПІДПРЕЄМСТВА

Кроль Е.М.
Державний університет телекомунікацій
м.Київ, Україна

Завантажити образ Kali Linux можна з офіційного сайту https://www.kali.org/. Хоча правильніше сказати, що тільки звідти його і можна завантажувати, щоб уникнути бонусного скачування, так би мовити, доповнень не передбачених розробником. На сайті доступні різні види образів, в тому числі можна скачати вже встановлену систему для віртуальних машин. Є образи з приставкою Light, це обрізаний варіант і використовувати його, без необхідності не варто, також можна вибрати образ з уже встановленим оточення робочого столу: Mate, Xfce, Kde. Хоча, при бажанні, їх можна буде встановити потім.

Ми візьмемо образ Kali Linux 64 Bit. Актуальна версія станом на момент написання статті 2019.1. Після скачування, образ потрібно записати на флешку якимось Rufus, після чого можна переходити безпосередньо до установки.

Для початку запускаємо з флешки і бачимо варіанти завантаження:
Вибираємо Graphical install, після чого потрібно вибрати мову:

Сьогодні Інтернет речей з його різномаїттям застосувань все глибше проникає в усі сфери нашого життя, доповнюючи звичні процеси у повсякденні та інноваційно вирішуючи сучасні питання бізнесу. За рахунок самої концепції Інтернету речей з’являється можливість покращувати якість нашого життя незнаними досі способами. Однак за високим попитом на подібні інновації стоїть відповідна кількість загроз, що несуть за собою пристрої Інтернету речей. Безпека Інтернету речей часто приноситься в жертву темпам виробництва нової «розумної» електроніки, а також часто не отримує достатньої уваги від розробників програмного забезпечення та виробників пристроїв і систем через відсутність або ж недостатнє фінансування для забезпечення необхідних перевірок до, у процесі, на фінальних стадіях розробки пристроїв та після виходу електроніки на ринок.

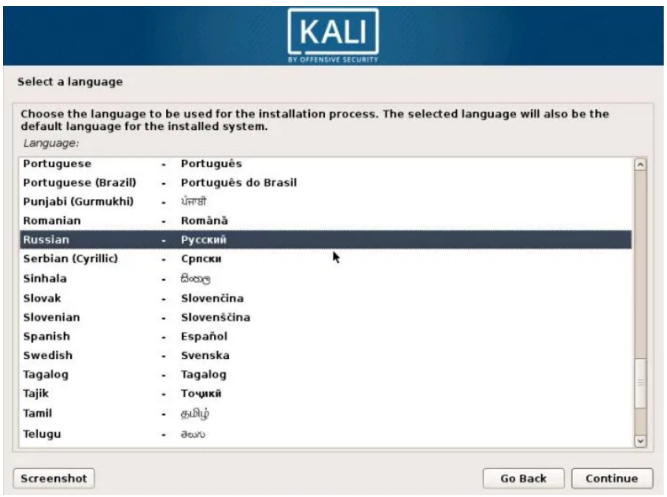


Рис.1. Завантаження Kali Linux

Хоча з огляду на гучні атаки за участю Інтернету речей обізнаність користувачів у технічному плані починає рости, питання безпеки пристроїв все ще може проходити повз уваги кінцевого користувача через велику кількість нових та зручних способів використання пристроїв, що підсвідомо віддаляє безпеку використання разом з конфіденціальністю даних та приватністю на другий план. Недоліки безпеки в пристроях Інтернету речей можуть призвести як до проблем з конфіденційністю та приватністю даних, так і до їх повної компрометації. В залежності від пристрою, вразливості також можуть спричинити великі фінансові збитки (створюються найпотужніші ботнети) або навіть пряму загрозу життю у випадку з біомедичним використанням IoT.

Недосконалі процеси розробки, тестування та імплементації кращих практик безпеки породжують недоліки і проблеми безпеки у розглянутих складових архітектури Інтернету речей та зумовлюють актуальність теми тестування на проникнення пристроїв Інтернету речей. Однак існуючі методології тестування на проникнення мають недоліки у випадку їх застосування до тестування пристроїв IoT: не враховується специфіка поверхні ата 15 ки пристроїв IoT, методики у сфері IoT висвітлюють процес тестування лише у контексті відповідності стандартам безпеки, що впливає на гнучкість тестування, не описується необхідний інструментарій та інші особливості тестування IoT. Через це виникає необхідність у вдосконаленні стандартів тестування шляхом розробки методу тестування безпеки пристроїв IoT. Мета роботи полягає в розробці методу тестування на проникнення пристроїв IoT з урахуванням особливостей даних систем. Об’єктом дослідження є тестування на проникнення пристроїв Інтернету речей.

Завдяки надійним утилітам, стабільності і простоті використання, це операційна система, з якою повинні бути знайомі все в IT-індустрії і комп'ютерні ентузіасти.

Використання тільки двох перерахованих вище додатків, значно допоможе в захисті інфраструктури інформаційних технологій. І Nmap, і Metasploit доступні на інших платформах, але їх простота використання і встановлена

\u200b\u200bконфігурація в Kali Linux роблять кращою операційною системою при оцінці і тестуванні безпеки мережі.

Як зазначалося раніше, будьте обережні при використанні Kali Linux, так як він повинен використовуватися тільки в мережевих середовищах, які ви контролюєте і маєте дозвіл на тестування.

Література

1. Основи використання Linux. *Путівник по Linux*. URL: https://linuxguide.rozh2sch.org.ua/.
2. 21 найкращих інструментів Kali Linux для злому та тестування на проникнення – WebSetNet. *WebSetNet*. URL: https://websetnet.net/uk/21-best-kali-linux-tools-for-hacking-and-penetration-testing/.

ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ВИТОКУ ЧУТЛИВОЇ ІНФОРМАЦІЇ ЗА МЕЖІ ПЕРИМЕТРУ КОРПОРАТИВНИХ МЕРЕЖ

Дорошин Б. В., Рабчун Д.І., к.т.н.
Державний університет телекомунікацій,
м.Київ, Україна

Згодом питання про захист чутливих даних (поняття що є “чутливими даними” всюди різниться, але у цій тезі ми будемо мати на увазі корпоративну, службову інформації, персональні дані користувачів, що користуються послугами цієї компанії і іншу інформацію, що може зашкодити умовній організації), що зберігаються, обмінюються у корпоративних мережах, повстане дуже гостро через невпинний технологічний прогрес, бо наявні наразі засоби хоч і забезпечують достатній рівень захисту, але у короткій-довгій перспективі вони можуть або ослабнути, або перестануть приносити той ефект, що був раніше, у результаті призводячи до фінансових та репутаційних втрат компанії, якій ці дані зберігає та використовує. Можна виділити деякі з найбільших витоків періоду 2010-2020х років , щоб визначити у чому частіше виникає проблема несанкціонованого поширення даних :

- Yahoo (2013) - у 2013 році хакери зламали систему Yahoo та вилили інформацію про клієнтів із понад 3 мільярдів облікових записів . На щастя, викрадені дані не включали такої важливої інформації, як платіжні дані, негешовані паролі або номери банківських рахунків.
- Facebook Inc. (2021) - У березні 2021 року хакери зламали найбільшу соціальну мережу Facebook за допомогою вразливості, яку було виправлено у 2019 році. На хакерському форумі було опубліковано колосальні 533 мільйони записів користувачів із 106 країн . До них входили повні імена, номери телефонів, місцезнаходження користувачів, біографічні відомості та адреси електронної пошти.
- SolarWinds (2020) - російські хакери, як кажуть, скомпрометували

SolarWinds, програмне забезпечення для моніторингу мережі, яке використовується Пентагоном, ядерними лабораторіями, спецслужбами та багатьма компаніями зі списку Fortune 500 (список з 500-та американських компаній, що мають найбільші прибутки). Цей злам стався через застарілий патч(оновлення) програмного забезпечення, який дозволив троянському коню для хакерів проникнути у систему SolarWinds. Ймовірно, виток складав п'ятдесят мільйонів записів невідомої кількості компаній і окремих осіб.

- Microsoft (2019) - 250 мільйонів записів клієнтів за 14 років було викладено без захисту паролем. Інформація містила адреси електронної пошти клієнтів, географічне розташування, запити у службу підтримки та обслуговування клієнтів, тощо. Базу даних почали розкривати 5 грудня 2019 року через збій у правилах безпеки та виправили 31 грудня 2019 року.

Як ми бачимо, в основному проблема витоків полягає саме у програмному забезпеченні, при цьому проявляється вона у вигляді необачності служби безпеки та співробітників, неправильного встановлення, налаштування, оновлення та використання ПЗ, хоча не можна і забувати про безсовісне використання слабкостями мережі співробітниками (інсайдерські атаки) або використання технічних каналів інформації, або навіть копіювання даних на електронний носій.

Система інформаційної безпеки містить у собі таку складову як захист від витоку інформації, вона ж data leak protection (DLP). Ця ж складова може представлятися як і окремі програмні(software) продукти, як і технічні(hardware) засоби, як і комбінація технічних та програмних засобів. Так як ми найчастіше зіштовхуємось зі зламами та інсайдерськими атаками, розглянемо саме програмні засоби.

DLP-системи зазвичай використовують три методи ідентифікації файлів, що містять чутливу інформацію: імовірнісний, детерміністський (визначає маркери “чутливих” даних) і комбінований.

Системи, що засновані на першому методі, здебільшого використовують лінгвістичний аналіз контенту і властивості файлів, тобто метадані. Ці системи доволі прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових-позитивних(false-positive) спрацьовувань.

Системи, що використовують детермінований підхід (маркери файлів), дуже надійні, але їм не вистачає гнучкості.

Комбінований підхід як зрозуміло поєднує обидва методи з аудитом середовища зберігання та обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації.

Є два основні підходи аналізу контенту. Перший підхід базується на фільтрації контенту, тобто змістовного наповнення інформації. Це означає, наприклад, що при перевірці на секретність стандартних офісних документів у форматі .docx, система спочатку переведе їх у текстовий формат, а потім, використовуючи заздалегідь підготовлені дані, зрозуміє до якого роду ці дані можна віднести. Контекстна ж фільтрація використовує інакший принцип : система перевіряє контекст, в якому передається інформація: витягує мітки

(маркери) файлу, дивиться на його розмір та/або аналізує поведінку користувача.

Щоб обрати продукт, який ми збираємося влаштувати у нашу мережу, ми використовуємо такі критерії оцінки, які вивела компанія Forrester :

1. Багатоканальність — тобто засіб має досліджувати різні канали, де може поширюватися чутлива інформація, як електронна пошта, веб-браузери, корпоративні чати, тощо.

2. Уніфікація — компоненти DLP мають бути зібрані в “одне єдине”, щоб ними можна було керувати з одного пристрою.

3. Активний захист — система має не тільки фіксувати, але й активно протидіяти витокам інформації.

4. Визначення змісту — система має розуміти як зміст, так і контекст даних, що знаходяться у мережі. Важливий не тільки вміст документу, але й контекст передачі, копіювання, тощо. Наприклад, відомості про клієнтів не мають бути у HR-менеджера і т.д. .

Наразі існує багато рішень від різних компаній, але найчастіше рекомендують саме від виробників антивірусного програмного забезпечення, так як загрози витоку нерідко супроводжуються встановленням шкідливого ПЗ, яке використовує вразливості мережі та кінцевих пристроїв для отримання несанкціонованого доступу до даних. Виділити можна таких виробників як :

- CoCoSys(Endpoint Protector) – одне з кращих рішень
- McAfee(McAfee DLP)
- ManageEngine(DataSecurity Plus)
- Digital Guardian
- Sophos
- Symantec (Symantec DLP) – теж виділяють як одне з найкращих рішень

Деякі з цих ПЗ мають величезний функціонал, але відповідно коштують дорого, інші ж мають менший функціонал, але мають помірну ціну або навіть є варіанти з пробним терміном, щоб спробувати програмний продукт.

У висновку хотів би зазначити, що захист чутливих даних є однією з невід’ємних частин всієї системи безпеки і взагалі будь-якої компанії, бо окрім фінансових втрат як і від самого витоку інформації, так і від групових судових позовів, це ще вплив на репутацію компанії, яка дає привід довіряти їй та користуватися її послугами. Американці завжди цінили більше репутацію, ніж фінанси, тому вони найбільш провідні спеціалісти з виробництва систем DLP. Хоч ці програмні засоби і є хорошими, але вони мають бути у тандемі з іншими програмами, обладнанням, що використовує організація, а також не варто забувати про роботу з персоналом, особливо їх навчанням та обізнаністю, поглядами на їх роботу, відносини з колегами і т.д.

Література

1. Integrity Systems URL: https://integritysys.com.ua/security/dlp/
2. Forrester URL: https://www.forrester.com/report/Now-Tech-Data-Loss-Prevention-Q1-2019/RES141687

3. Termly URL: https://termly.io/resources/articles/biggest-data-breaches/
4. Software Testing Help URL: https://www.softwaretestinghelp.com/data-loss-prevention-software/

СЕКЦІЯ 5. ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ

СИСТЕМИ МОНІТОРИНГУ ДЛЯ ВИЯВЛЕННЯ ТА ПРОТИДІЇ СУЧАСНИМ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Яцковський В. В.
Державний університет телекомунікацій
м. Київ, Україна

На сьогоднішній день існує багато загроз інформаційній безпеці для підприємств. Кожне підприємство має одну або декілька мереж, які потрібно захищати від інформаційних загроз. Для цього використовуються різноманітні методи та засоби захисту мережевої інфраструктури, як приклад: міжмережеві екрани (WAF, NGFW), системи запобігання та виявлення вторгнень (IPS/IDS), засоби контролю привілейованих користувачів (PAM) тощо.

При такій великій кількості різноманітних систем та компонентів в мережі стає складно слідкувати за кожним з них окремо, збирати та аналізувати дані. Для того, щоб моніторити й аналізувати все централізовано, використовують різні моніторингові системи, зокрема системи управління інформацією та подіями інформаційної безпеки - SIEM (Security Information and Event Management).

SIEM об'єднує в собі функції управління інформацією безпеки SIM (Security information management) та управління подіями безпеки SEM (Security Event Management) і збирає відомості про всю мережеву активність в одному місці у вигляді зрозумілого набору даних.

На думку фахівців IBM [1], основними перевагами SIEM є:

- Розширене розпізнавання загроз у режимі реального часу;
- Аудит відповідності нормативним вимогам;
- Автоматизація на основі штучного інтелекту;
- Підвищення організаційної ефективності;
- Виявлення актуальних та невідомих загроз;
- Проведення цифрових криміналістичних розслідувань;
- Оцінювання та звітування про відповідність нормативним вимогам;
- Моніторинг користувачів і додатків.

SIEM системи працюють шляхом збирання логів та потоків даних з різних джерел. Такими джерелами можуть слугувати: програмне забезпечення, антивіруси, міжмережеві екрани, мережеве обладнання, хмарні середовища, програмне забезпечення, сервера.

Далі система проводиить агрегацію та нормалізацію зібраних даних для подальшого їх аналізу на предмет аномалій і загроз, встановлення тенденцій. Також SIEM досліджує спрацювання, виявляє порушення; звітує про ризики і невідповідності вимогам безпеки.

SIEM виявляє закономірності та аномальну поведінку, тому, навіть якщо окрема подія не викликає тривоги, SIEM може виявити взаємозв'язок між кількома подіями, які в іншому випадку залишилися б непоміченими, і спровокувати спрацювання. Також SIEM зберігає ці журнали в базі даних, що дозволить проводити більш глибокі криміналістичні розслідування [2].

Отже, SIEM допомагає аналітикам безпеки швидше та якісніше аналізувати події та інциденти інформаційної безпеки, збираючи інформацію з великої кількості компонентів IT-інфраструктури підприємства. Треба зазначити, що SIEM система напряму не протидіє хакерам, а збирає, агрегує, нормалізує та корелює дані, надаючи аналітику повноцінне розуміння того що відбувається всередині IT-інфраструктури.

Література

1. Security information and event management (SIEM) explained. URL: https://www.ibm.com/topics/siem
2. What Is Security Information and Event Management (SIEM)? URL: https://www.splunk.com/en_us/data-insider/what-is-siem.html

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОРГАНІЗАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Колесник П.В., Мужанова Т.М., к.держ.упр., доц.
Державний університет телекомунікацій
м. Київ, Україна

Глобальна мережа Інтернет відкриває широкі можливості для пошуку інформації, спілкування, навчання, роботи та відпочинку. У той же час Інтернет є величезною щоденно зростаючою базою даних про користувачів, в отриманні доступу до якої дуже зацікавлені зловмисники. Саме про це свідчить статистика, відповідно до якої кількість Інтернет-загроз, спрямованих проти інформації, зростає пропорційно до загальної кількості продукованих даних [1].

Існує два основні види загроз в Інтернеті, які можуть негативно вплинути на інформаційну безпеку організації, в тому числі її персоналу, третіх сторін, клієнтів і зацікавленої громадськості: технічні і соціальні [2].

Основними технічними загрозами для користувачів є шкідливі програми, DoS та DDoS-атаки.

Шкідливі програми. Мета шкідливих програм – завдати шкоди комп'ютеру, серверу чи комп'ютерній мережі: пошкодити, викрасти або знищити дані, що зберігаються на комп'ютері, уповільнити або повністю зупинити роботу пристрою.

До шкідливих програм належать віруси, черв'яки, троянські програми, різновиди та функціонал яких постійно вдосконалюються. З кожним роком зростає кількість організацій та окремих осіб, які постраждали від програм-

вимагачів. Так, у 2021-22 роках 60% організацій, які стали жертвами їхніх атак, змушені були заплатити зловмисникам [1].

DoS та DDoS атаки. Найбільш поширеними загрозами, спрямованими проти доступності інформації є атаки типу «Відмова в обслуговуванні», масштаби і складність яких збільшуються з кожним днем. У більшості випадків такі атаки реалізуються мережею ботнетів, що дозволяє підвищити охоплення і потужність нападу. Крім традиційних завдань щодо виснаження інформаційних ресурсів, зниження продуктивності ІКС, витоку даних і збоїв у роботі технічних пристроїв DDoS поступово зосереджуються на реалізації мобільних і сенсорних сценаріїв, де доступність пристроїв і датчиків знижується внаслідок збільшення споживання заряду батареї.

Про зростання потужності таких загроз свідчить той факт, що найбільша HTTP DDoS-атака обсягом понад 70 млн запитів за секунду (rps), яка була зареєстрована у лютому 2023 року, перевищила попередній рекорд у 46 млн запитів за секунду у червні 2022 року на 35% [3].

Основними соціальними загрозами інформаційній безпеці в мережі є використання різноманітних методів соціальної інженерії.

Фішинг. Згідно з DBIR Verizon за 2021 рік, понад 80% усіх витоків даних є наслідком використання методів соціальної інженерії, з них близько 25% - пов’язані з виманюванням конфіденційних даних, тобто фішингом [4].

Метою фішингових атак є отримання доступу до конфіденційних даних (адреса, номери телефону і кредитних карток, логіни та паролі), з використанням підроблених веб-сторінок, а основним мотивом їхніх організаторів - отримання матеріальної вигоди.

Як свідчить статистика, поряд із традиційним фішингом з’являються нові цільові (таргетовані) форми, такі як spear-phishing, whaling, smishing і vishing [1]. Такі атаки спрямовані на конкретного користувача, який нерідко є представником топ-менеджменту компанії чи особою, яка приймає важливі рішення. Спочатку зловмисник збирає детальну інформацію про свою жертву, включаючи деталі її роботи та людей, з якими вона регулярно спілкується, а потім надсилає дуже персоналізований електронний лист. Таке повідомлення не викликає підозр, а, отже його значно складніше ідентифікувати як шкідливе.

Фальшиві антивіруси та програми для забезпечення безпеки. Зловмисники часто розповсюджують шкідливі програми під виглядом антивірусів. Ці програми генерують повідомлення, які зазвичай містять попередження про те, що комп'ютер нібито заражений, і рекомендують пройти за вказаним посиланням для успішного лікування, завантаживши й запустивши файл оновлення. Джерелами поширення хибних антивірусів є електронна пошта, соціальні мережі та навіть спливаючі вікна на комп'ютері, які імітують системні повідомлення.

Підміна зворотної адреси. Оскільки злочинці добре знайомі з особливостями людської психіки, їм добре відомо, що користувачі набагато більше довіряють повідомленням, отриманим від знайомих, і з більшою ймовірністю відкриють їх, не чекаючи підступу. Тому зловмисники підробляють зворотну адресу на знайому користувачеві, щоб обманом заманити його на сайт,

який містить шкідливу програму, або дізнатися персональні дані. Жертвами власної довірливості часто стають клієнти Інтернет-банків.

Засоби захисту від загроз в Інтернеті. Для того щоб зменшити ризик організації стати жертвою технічних атак, необхідно дотримуватися нескладних правил: впровадити і забезпечити дотримання політики «сильних» паролів, регулярно та своєчасно оновлювати програмне забезпечення, завантажуючи усі програми тільки з сайтів компаній-виробників.

Завдання щодо протидії DDoS-атакам є значно важчим, і робота щодо захисту хостингу має починатися ще на етапі проектування мережі й запуску серверів. Також важливим є постійний моніторинг трафіку й визначення невластивих йому відхилень, що є однією зі складових захисту сервера від DDoS-атак. Найбільш високопродуктивним і ефективним вважається застосування технічних систем розподіленого захисту [5].

Важливим і ефективним засобом запобігання як технічним, так і соціальним загрозам інформаційній безпеці в Інтернеті є впровадження програм інформування та навчання персоналу, в рамках якої працівники регулярно отримують найновішу інформацію про методи й технології реалізації загроз в Інтернеті, навчаються виявляти і протидіяти деструктивним впливам. Важливим завданням організації є формування культури безпечної поведінки у всесвітній мережі й дотримання вимог інформаційної безпеки. Також доцільно використовувати засоби контролю й моніторингу поведінки персоналу.

Отже, загрози інформаційній безпеці організації в мережі поділяють на технічні й соціальні. Найбільш поширеними технічними загрозами є шкідливе програмне забезпечення, в тому числі програми-вимагачі, а також DoS та DDoS-атаки. Основою більшості соціальних загроз інформаційній безпеці в мережі є використання різноманітних методів соціальної інженерії, в тому числі фішинг, якому сьогодні притаманна спрямованість на вузьку цільову аудиторію.

Для запобігання і протидії загрозам інформаційній безпеці в Інтернеті організації доцільно комплексно використовувати як програмно-технічні засоби, так і методи роботи з персоналом.

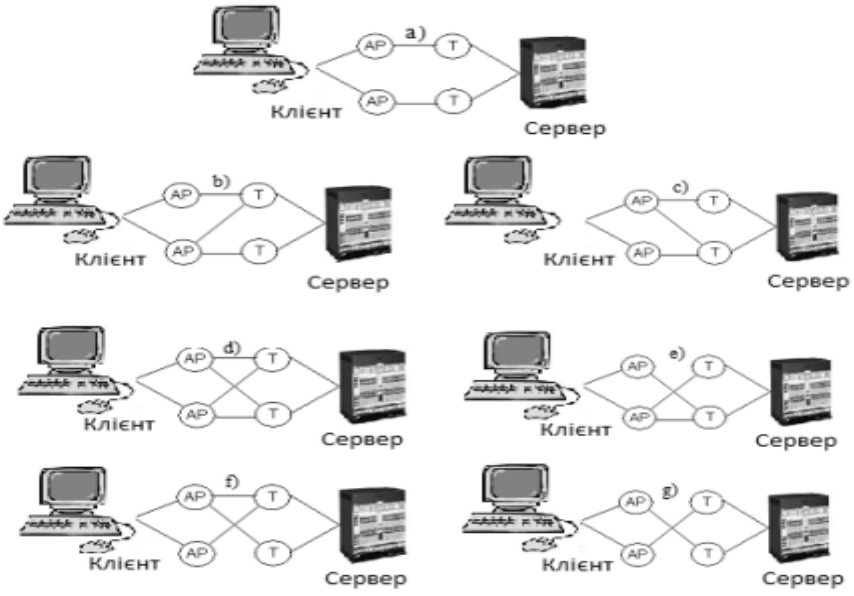
Література

1. The ENISA Threat Landscape 2022. Jctober 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
2. Черних О.О. Аналіз класифікацій загроз в Інтернеті. *Вісник ЛНУ імені Тараса Шевченка*. № 1 (290), 2015. С. 281-289.
3. Колонович К. Cloudflare зупинила рекордну DDoS-атаку у 71 мільйон запитів за секунду. URL: https://speka.media/cloudflare-zupinila-rekordnu-ddos-ataku-u-71-milion-zapitiv-za-sekundu-pno879
4. Verizon Data Breach Investigations Report 2021. Social engineering. URL: https://www.verizon.com/business/resources/reports/dbir/2021/incident-classification-patterns/social-engineering/
5. Захист від DDOS-атак. URL: https://iitd.com.ua/zashchita-ot-ddos-atak/

МЕТОДИ ОЦІНЮВАННЯ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДО РОЗПОДІЛЕНИХ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ (DDOS)

Савельєв О.А.
Державний університет телекомунікацій
м. Київ, Україна

Метою роботи є розроблення та вивчення формалізованої математичної моделі класу атак DoS/DDoS з урахуванням структури мережі та вагових коефіцієнтів міри впливу кожного виду атак, що дасть змогу ефективно проектувати системи захисту інформації у КМ із урахуванням інформаційних загроз. Для того, щоб з'ясувати ключові задачі архітектури, стійкої до нападу КМ, спочатку розглянемо спрощену модель комунікації клієнт-сервер, яка зображена на рисунку 1.



Модель комунікації клієнт-сервер:
AP – точка доступу, T – точка призначення

Рис. 1. Модель комунікації клієнт-сервер

У цих моделях обмежимося двома точками входу й двома точками призначення. Лінії, що сполучають точки входу й точки призначення, моделюють комунікацію між ними в КМ.

Під стійкістю мережі розуміють здатність мережі забезпечити альтернативну комунікацію під час зруйнування (чи спроб зруйнувати) хоча б одного шляху між клієнтом і сервером.

У результаті аналізу класифікації DoS/DDoS/-атак ми запропонували формалізовану математичну модель, яка дає змогу визначити рівень впливу показників атак на КМ.

Ґрунтуючись на класифікації інформаційних загроз, характерних для атак типу DoS/DDoS, запропоновано формалізовані моделі лінійного виду для диференціації атак на основі методу вагових коефіцієнтів. За допомогою цих показників та коефіцієнтів можна визначити основні види загроз у КМ, що дають змогу ефективно проектувати системи захисту інформації із урахуванням інформаційних загроз.

Для того, щоб спроектувати мережу з урахуванням усіх інформаційних загроз, слід враховувати як вагові коефіцієнти різних видів атак, так і захищеність компонентів КМ від внутрішніх та зовнішніх атак.

Література

1. Антонюк А. О. Основи захисту інформації в автоматизованих системах : Навч. посіб. Київ : КМ Акад., 2003. 244 с.
2. Атаки на відмову в обслуговуванні комп’ютерних мереж / М. П. Карпінський та ін. *Комп'ютерні системи та мережі*. 2014. № 806. С. 94–99. URL: https://ena.lpnu.ua/handle/ntb/27243.

РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Легомінова С.В., д.е.н., проф., Святська Н. А.
Державний університет телекомунікацій
м. Київ, Україна

Сфера розробки кібербезпеки значно зросла за останнє десятиліття, оскільки все більше організацій визнають необхідність інвестувати в технологічні рішення для захисту від кіберзагроз. Для успішного впровадження системи управління кібербезпекою необхідно її розробити відповідно до потреб, для чого потрібно знати інструменти проектування.

Цифрова ера принесла різноманітні переваги організаціям і окремим особам. Інформаційні технології щодня набувають все більшого поширення. Оскільки мережі та комп’ютерні системи стають поширеними, уразливі місця, недоліки, загрози безпеці та ризики зростають швидше, ніж у багатьох інших технологіях. Види загроз різноманітні. Фахівці та експерти з безпеки намагаються створити рішення для кожного типу загроз за допомогою різних методів, таких як сигнатури атак і евристичних підходів для запобігання. Однак у міру створення рішень з’являються нові типи загроз, такі як спам, шпигунське програмне забезпечення, рекламне програмне забезпечення, черв’яки та трояни. Незважаючи на те, що уряди приймають закони та нормативні акти для мінімізації так званих «цифрових злочинів», їх природа і цифрове середовище робить майже неможливим зловити зловмисників.

Проблема управління безпекою має багато аспектів. Найважливішим є комплексність. Чим більше створюється та використовується складне та якісне програмне забезпечення, тим більше уразливостей виникає. Крім того, існує

багато хакерів або зломщиків, які виявляють ці вразливості та використовують їх. У хакерів кілька мотивів: одні шукають слави та грошей, інші роблять це просто з цікавості. Однак наслідки атак, незалежно від мотивів зловмисників, завжди обходяться організаціям дорого.

Заходи безпеки в комп'ютерних системах впливають на зручність використання систем. У разі застосування посилення безпеки користувачі втрачають одну або кілька функціональних можливостей, або стає важче виконати завдання чи отримати доступ до файлу в Інтернеті [1, С. 1-5].

Безпека зазвичай суперечить зручності систем. Користувачі віддадуть перевагу легкому, але небезпечному способу ніж складному, але безпечному. Природа безпеки ускладнює адміністрування безпеки, оскільки користувачі не орієнтовані на безпеку за замовчуванням.

Інжиніринг кібербезпеки — це застосування інженерних принципів і практик для проектування, розробки, впровадження та управління безпечними комп'ютерними системами. Він включає широкий спектр заходів, таких як проектування захищених мереж і систем автентифікації, розробка криптографічних алгоритмів, написання безпечного коду, аналіз ризиків безпеки системи, тестування системних уразливостей і впровадження заходів безпеки. Інженери з кібербезпеки відповідають за забезпечення стійкості інформаційних систем у середовищі, де зловмисники постійно шукають способи використати слабкі місця або отримати доступ до конфіденційної інформації. Вони використовують свої знання обчислювальних технологій, щоб захистити дані від несанкціонованого доступу та потенційного пошкодження [3].

Окрім технічних знань і досвіду, успішні інженери з кібербезпеки демонструють потужні навички вирішення проблем і відмінні комунікаційні навички. Вони повинні вміти швидко й точно аналізувати складні ситуації, а потім пояснювати свої висновки в стислій та зрозумілій формі. Вони також повинні вміти співпрацювати з іншими членами команди, щоб забезпечити врахування всіх аспектів безпеки системи.

Інструменти проектування включають креслення, специфікації, міждисциплінарну координацію, вибір продукту, управління проектами та управління клієнтами.

Креслення - це серце дизайну. Воно повинно показувати наступне: зв'язок пристроїв із їхнім фізичним середовищем, взаємозв'язок пристроїв із системою трубопроводів і потужністю, зв'язок пристроїв один з одним відношення пристроїв до користувача [2, chapter 10].

Якщо креслення — це серце дизайну, то специфікації — це голова. Специфікації зазвичай мають прецедент у судових спорах. Креслення призначено лише для ілюстрації стандартів і практик, зазначених у специфікаціях. Багато проблем з укладанням контрактів про систему безпеки є результатом неповних або неправильних специфікацій. Специфікації повинні містити опис того, що передбачає проект; описи всієї інтегрованої системи та кожної підсистеми; опис послуг, які надаватиме підрядник; а також перелік

прийнятних продуктів і прийнятних практик встановлення, тестування, приймання, навчання та гарантії[2, chapter 4].

Вибір продукту не менш важливий інструмент проектування. Вказавши правильні продукти для роботи, можна створити чудову систему, яка легко перевершить очікування власника. Неправильна продукція може спричинити проблеми в функціоналі системи.

Інженер повинен керувати розробницькою частиною проекту. Управління проектом полягає в створенні системи, яка відповідає потребам клієнта, потребам інтегратора та потребам керівника проекту клієнта. Все це інженер повинен робити під час роботи над іншими проектами; він або вона має надати результати проекту вчасно та повністю, щоб усі сторони були задоволені. Управління проектом має чотири основні фази: ініціювання проекту, планування проекту, виконання проекту, контроль та закриття проекту.

Отже, безпека мережевих та інформаційних систем вважається ключовою проблемою в спробах зберегти функціонування та безпеку цифрової економіки в найближчому майбутньому. Система управління безпекою надає ефективний функціонал, який буде допомагати протистояти ризикам, а для того, щоб ця система працювала було розглянуто низку інструментів для розробки потрібної системи менеджменту інформаційної безпеки.

Література

1. Hulusi Önder (July 2007). A security management system design. URL: https://etd.lib.metu.edu.tr/upload/12608515/index.pdf
2. Thomas L. (September 2014). Norman. Integrated Security Systems Design, 2nd Edition. Chapters 4, 10. URL: https://learning.oreilly.com/library/view/integrated-security-systems/9780128000229/B9780128000229000048.xhtml#s0010
3. Розробка кібербезпеки: визначення, стандарти та методи. URL: https://visuresolutions.com/uk/blog/cybersecurity-engineering

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ ІНТЕРНЕТ-МАГАЗИНУ

Сковерко В. І.
Державний Університет Телекомунікацій
Київ, Україна

На сьогоднішній день неможливо уявити, компанію, що не має представництва в інтернеті, а саме – свого веб-сайту. Навіть будь-яка людина може створити свій сайт-візитку чи інформаційну сторінку, блог чи форум, інтернет-магазин чи будь-який інший інтернет-ресурс.

У зв’язку з поширенням нових технологій з’являються і нові загрози.

Коли клієнти роблять покупки на вашому сайті, вони довіряють вам конфіденційну інформацію кожного разу, коли роблять замовлення. Це включає

такі дані, як: ім’я користувача, реквізити банківського рахунку, його місцезнаходження.

Основні пункти у забезпечення безпеки інтернет магазину:

- Шифрування HTTPS. Найкраще захистити канали зв’язку на вашому веб-сайті за допомогою протоколу SSL. Це дозволяє безпечно передавати конфіденційні дані клієнтів із домену користувача на домен вашого сервера.
- Брандмауери. Вони призначені для обмеження вхідного та вихідного зв’язку необхідними протоколами (наприклад, SSH, HTTP та HTTPS).
- Правила паролів для облікових записів користувачів. Варто встановіть такі параметри, як мінімальна довжина пароля та використання великих і малих літер, щоб зменшити ризик злому хакерів в обліковий запис клієнта та отримання доступу до його конфіденційних даних.
- Регулярне резервне копіювання. Якщо ваш сервер зламано, ви не зможете отримати до нього доступ. Тоді дуже важливо мати повну резервну копію для відновлення.
- Оновлення всього програмного забезпечення у своїй структурі. Наприклад операційна система, веб-сервер, база даних MySQL.
- Подбати про технічний захист обладнання: захист від зовнішніх подразників, волога, пилюка; забезпечення енергопостачання охолодження, та відмовостійкості обладнання.

З боку правового регулювання подібної діяльності в Україні передбачені закони: “ Про захист інформації в інформаційно-комунікаційних системах”, та “ Про захист персональних даних”.

У цих законах передбачено відносини у сфері захисту інформації в інформаційно-телекомунікаційних системах та відповідальність за порушення закону.

Література

1. Безпека інтернет-магазину URL: https://www.mollie.com/gb/growth/webshop-security
2. Безпека інтернет-магазину, що і чому потрібно захищати URL: https://rau.ua/novyni/bezopasnost-internet-magazina-chto-i-pochemu-nuzhno-zashhishhat/
3. Закон України “Про захист інформації в інформаційно-комунікаційних системах” URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
4. Закон України “Про захист персональних даних” URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

ЗАПОБІГАННЯ І ПРОТИДІЯ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Вакуленко Т.Р.
Державний університет телекомунікацій
м.Київ, Україна

Соціальна інженерія – це складний механізм впливу на людину, що містить елементи маніпулювання та психологічного тиску.

Одним з методів соціальної інженерії є фішинг, що полягає у використанні підробленого електронного листа або веб-сайту з метою вибудовування довіри та здобуття конфіденційної інформації.

На підприємствах необхідно проводити навчання співробітників з питань кібербезпеки та соціальної інженерії з метою зменшення ризику використання методів соціальної інженерії.

Створення культури кібербезпеки на підприємстві може допомогти зменшити ризик використання методів соціальної інженерії.

Існує ряд технічних заходів для запобігання фішингу, таких як використання анти-спаму та анти-вірусного програмного забезпечення, фільтрація електронної пошти та використання захисних механізмів веб-браузера.

Важливо встановити процедуру підтвердження автентичності запитів на інформацію або трансакції для зменшення ризику використання методів соціальної інженерії, таких як імітація підроблених листів або підроблення переказів.

Важливо використовувати двофакторну аутентифікацію для зменшення ризику використання методів соціальної інженерії, які спрямовані на викрадення паролів або доступу до облікових записів користувачів.

Важливо вести моніторинг інформаційної безпеки та вживати заходів для забезпечення конфіденційності, цілісності та доступності інформації на підприємстві.

Важливо встановити процедуру повідомлення про підозрілі активності або інциденти інформаційної безпеки для швидкого реагування та зменшення наслідків інцидентів.

Важливо встановити обмеження доступу до конфіденційної інформації та здійснювати періодичну перевірку прав доступу користувачів.

Література

1. Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.
2. Sheng, S., Holbrook, M., & Kumaraguru, P. (2011). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems pp. 373-382.

3. Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ МЕРЕЖЕВИХ ЕКРАНІВ ТА ФІЛЬТРІВ ДЛЯ ПРОТИДІЇ КІБЕРАТАКАМ

Мунтян М.Р., Рабчун Д.І., к.т.н.
Державний університет телекомунікацій
м. Київ, Україна

З розвитком інформаційно-комунікаційних засобів, в тому числі глобальної мережі Інтернет, зростає значення захисту процесів передачі інформації. Особливо критично питання мережевої безпеки постало під час повномасштабного вторгнення РФ. Державні установи та компанії потерпають від організованих кібератак, більша частина з яких мають чітку мету: посіяти серед населення паніку та деморалізувати його.

У даній ситуації найнебезпечнішим є недооцінювання сил і можливостей ворога, а також недостатня якість або відсутність аналізу інцидентів інформаційної та кібербезпеки.

Як зазначили фахівці команди реагування на комп'ютерні надзвичайні події України CERT-UA, у переважній більшості інцидентів початковою точкою компрометації є публічна інформаційна система з неоновленим і/або налаштованим за замовчанням програмним забезпеченням (поштовий сервер, VPN-сервер, веб-сервер, система управління контентом (CMS) веб-сайту, СУБД тощо) [1].

Таким чином, будь-який вектор атаки на мережу, найчастіше віддаленої, власне проходить через мережу Інтернет, а отже критичним є забезпечення захищеності таких мережевих ресурсів.

На нашу думку, ефективною у протидії мережевим атакам різних рівнів (мається на увазі рівні 1-7 стеку OSI) є архітектура, яка включає такі компоненти:

1. Мережевий екран (Firewall). Як свідчить практика, найширшого застосування отримали рішення NGFW (Next Generation FireWall). Як і нижче перелічені засоби, мережеві екрани можуть бути «залізними» (програмно-апаратне рішення) або «хмарними» рішеннями.

Особливість сучасних NGFW полягає у можливості їх гнучкого налаштування та інтеграції з іншими рішеннями, щоб покрити питання захисту від витоків даних (DLP), налаштування захищеного віддаленого доступу та криптографічного захисту трафіку, шифрування носіїв даних тощо. Ці можливості можуть бути активованими у самому продукті або інтегровані через інший продукт.

2. Мережевий екран ВЕБ-додатків (WAF). WAF-фаєрволи спроектовані спеціально для аналізу пакетів на прикладному (7) рівні, оскільки NGFW оперує

на більш низьких 1-4 рівнях OSI і не підходить для захисту ВЕБ-сервісів (HTTP-протокол є одним із протоколів 7-го рівня).

Найвідомішими мережевими атаками є SQL-ін'єкції, XSS-атаки, DDoS. Повний перелік актуальних векторів атак щорічно формується спільнотою OWASP [2]. Від таких атак і налаштовується захист на базі WAF.

3. Системи поштових мережевих екранів – засоби фільтрації пошти, що дозволяють відсіювати фішинг-розсилки, спам або листи із шкідливими файлами.

Без впровадження згаданих систем не можна вважати реалізацію корпоративної мережі успішною, не кажучи вже про забезпечення її безпечного функціонування.

Після активації правил, які налаштовані за замовчуванням на тій самій Imperva Cloud WAF уже можна попередити сканування веб-ресурсів базовими сканерами. Якраз такої активності найбільше у всесвітньому трафіку, в якому здійснюється безперервне сканування усіх можливих мережевих девайсів.

Варто зазначити, що останні атаки на державні установи показали, що захист інформації не обмежується лише технічними засобами, а включали також використання методів соціальної інженерії (зловмисне ПЗ завантажувалося через вкладення у листах). Це додатково підтверджує критично важливу роль застосування мережевих фаєрволів різних типів і використання антивірусного захисту.

Таким чином, для захисту локальних мережевих ресурсів і публічних сервісів (якщо такі є) недостатнім є просте налаштування програмних і програмно-апаратних засобів. Необхідно проводити повну конфігурацію мережевих екранів з урахуванням специфіки ресурсів, що захищаються. Крім цього, правильне налаштування мережевого обладнання і систем забезпечення мережевого захисту значно зменшує вплив людського фактору на захищеність інформаційно-телекомунікаційних систем.

Література

1. Щодо невідкладних заходів кіберзахисту. URL: https://cert.gov.ua/article/1751036

2. OWASP Top Ten 2021. URL: https://owasp.org/www-project-top-ten/

СЕКЦІЯ 6. БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ

ФАКТОРИ, ЯКІ ВПЛИВАЮТЬ НА СТАН КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ляшенко О.М.
Національний університет оборони України
імені Івана Черняховського
м. Київ, Україна

У сучасному суспільстві кібератаки стають частішими та мають тенденцію чинити все значніший і триваліший вплив на економіку країни, незаперечним є той факт, що надійний захист від кібератак активно впливає на стан економічної, політичної, соціальної, оборонної та інших складових національної безпеки держави.

Очевидним є той факт, що порушення функціонування об'єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великого матеріального, фінансового, економічного збитку або великомасштабними порушеннями життєдіяльності міст та населених пунктів. У цих умовах надзвичайно важливу роль відіграє забезпечення безпеки, у тому числі і кібербезпеки об'єктів критичної інфраструктури держави.

Враховуючи зазначене вище, метою тез є визначення основних факторів, що впливають на стан кібербезпеки об'єктів критичної інфраструктури.

Проведений аналіз існуючих систем захисту інформації, дає змогу визначити основні складові частини системи кіберзахисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури:

- нормативно-правова;
- організаційна;
- технічна;
- підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки ІТС ОКІ.

ІТС зазвичай являються об'єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об'єкти захисту від кіберзагроз.

Кіберзагрози для ІТС можуть виходити з різних джерел: навмисних, ненавмисних, природних.

Джерела кібератак для інформаційних систем об’єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини.

Відповідно проведеного аналізу, на стан забезпечення кібербезпеки ІТС об’єкта критичної інфраструктури можуть впливають такі фактори:

- наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки ІТС об’єктів критичної інфраструктури;
- наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;
- наявність вразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;
- наявність чи відсутність сприятливих умов для реалізації кіберзагроз;
- привабливість активів, на які власне і спрямовуються кібератаки;
- наслідки від можливої реалізації кіберзагроз;

Також, одним із таких показників може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.

Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, об’єкти сектору безпеки і оборони, відомства, дипломатичні установи тощо.

Таким чином, кібербезпека є невід'ємною складовою інформаційної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної та інформаційно-технологічної безпеки держави.

Література

1. Franke U. War by non-military means: understanding Russian information warfare : монографія. Stockholm : Totalförsvarets Forskningsinstitut (FOI), 2015. 63 p.
URL: https://dataspace.princeton.edu/bitstream/88435/dsp019c67wq22q/1/foir_4065.pdf.
2. Darczewska J. Anatomia rosyjskiej wojny informacyjnej: Operacja krymska--studium przypadku = The anatomy of Russian information warfare : the Crimean operation, a case study. Warszawa : Ośrodek Studiów Wschodnich im. Marka Karpia, 2014. 36 p.

БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (БАНКИ)

Каблучко Д.М.
Державний університет телекомунікацій
м.Київ, Україна

У сучасному світі на сьогоднішній день проблема забезпечення інформаційної безпеки об'єктів критичної інфраструктури і, зокрема, банків є важливою. Діяльність захисту інформації набирає обертів у всіх сферах життєдіяльності суспільства, не залишається осторонь і банківська сфера. У наш час цінність інформації, що зберігається в банках, багаторазово зросла, а, отже, забезпечення інформаційної безпеки банку - запорука забезпечення захисту всіх його інформаційних активів.

У наші дні у зв'язку із загальною інформатизацією та комп'ютеризацією банківської діяльності значення інформаційної безпеки банків багаторазово зросло. Ще 30 років тому об'єктом інформаційних атак були дані клієнтів банків або діяльність самого банку. Тоді такі атаки були рідкісними, коло їхніх замовників було дуже вузьким, а збитки могли бути значними лише в особливих випадках. В даний час в результаті повсюдного поширення електронних платежів, пластикових карток, комп'ютерних мереж, популярності послуг, що надають клієнтам за допомогою Інтернет-технологій, об'єктом інформаційних атак стали безпосередньо кошти як банків, так і їх клієнтів. Здійснити спробу розкрадання може будь-хто – потрібна лише наявність комп'ютера, підключеного до мережі Інтернет. Причому для цього не потрібно фізично проникати до банку, можна «працювати» і за тисячі кілометрів від нього.

Свій розвиток банківська справа розпочала з найдавніших часів, і проаналізувавши історію, очевидно, що люди завжди прагнули убезпечити свої заощадження. Однак у ті часи проконтролювати збереження своїх вкладів було набагато простіше, ніж зараз у століття розвитку інформаційних технологій, адже сьогодні зловмисник, може навіть не вриваючись у банк, викрасти найважливішу інформацію.

Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці співробітників банку, запровадити нові фінансові продукти та технології. Однак прогрес у техніці злочинів йшов не менш швидкими темпами, ніж розвиток банківських технологій. В даний час понад 90% всіх злочинів у цій сфері пов'язані з використанням автоматизованих систем обробки інформації банку (АСОІБ). Отже, при створенні та модернізації АСОІБ банкам необхідно приділяти пильну увагу забезпеченню її безпеки [1, с. 8–9].

Будь-яка загроза, спрямована на безпеку банку, перш за все спрямована на виведення фінансових активів або заволодіння конфіденційною інформацією. Витік інформації з банку - це безперечно фінансові збитки для бізнесу. Розглянемо деякі види важливої інформації для банку і який ризик вони можуть завдати для установи при попаданні до зловмисника:

- внутрішні документи банку – небезпека різних зовнішніх атак;

• персональні дані клієнтів – втрата клієнтів, судові розгляди через порушення закону;

• плани виведення нової пропозиції ринку- конкуренти зможуть реалізувати товар швидше;

• інформація про фінансову діяльність – втрата інвестиційної привабливості у клієнтів;

• відомості про партнерів та умови співпраці – конкуренти запропонують кращі.

У будь-якому випадку збитки будуть або фінансовою втратою, або втратою клієнтів, або погіршенням репутації банку, або винесенням штрафних санкцій у відповідність до законодавства, а за найгіршого результату вся сукупність завданих збитків може призвести до закриття банку взагалі.

Так, виходячи з усіх можливих загроз та особливостей інформаційних систем банку, банк повинен мати мережу банкоматів, систему онлайн-банкінгу, пивинен робити заходи, необхідні для забезпечення інформаційної безпеки кредитно-фінансової установи. У банківських системах містяться дані про фінансові операції, які проводяться клієнтами, їх персональні дані та дані про рахунки. Особлива важливість захисту даної інформації для банку очевидна, але без ретельно продуманої системи обробки, передачі та зберігання банківської інформації буде неможливим.

Для забезпечення безпеки банку необхідно створити цілу структуру, яка зможе комплексно захистити конфіденційну інформацію про клієнтів та всі банківські дані в цілому. Можна виділити загальну послідовність заходів, яка допоможе організувати структуру захисту:

- визначення інформації, що захищається;
- створення та налагодження комплексної системи захисту;
- постійний контроль та удосконалення вжитих заходів.

Відомі різні варіанти захисту інформації - від охоронця на вході до математично вивірених способів приховування даних від проникнення. Крім того, можна говорити про глобальний захист та його окремі аспекти: захист персональних комп'ютерів, мереж, баз даних та ін.

Слід зазначити, що абсолютно захищених систем немає. Можна говорити про надійність системи, по-перше, лише з певною ймовірністю, а по-друге, про захист від певної категорії порушників. Проте проникнення в комп'ютерну систему можна передбачити. Захист – це свого роду змагання оборони та нападу: хто більше знає та передбачає дієві заходи, той і виграв.

Сучасний банк важко уявити без автоматизованої інформаційної системи. Комп'ютер на столі банківського службовця вже давно перетворився на звичний та необхідний інструмент. Зв'язок комп'ютерів між собою і з потужнішими комп'ютерами, а також з ЕОМ інших банків - також необхідна умова успішної діяльності банку: дуже велика кількість операцій, які необхідно виконати протягом короткого періоду часу .

Комп'ютерні системи, без яких не може обійтися жоден сучасний банк, є джерелом абсолютно нових, раніше невідомих загроз. Більшість із них

обумовлено використанням у банківській справі нових інформаційних технологій і характерні не лише для банків.

У висновку, хотілося б зазначити, що за безпеку даних клієнтів банків відповідає не тільки якісно створена система інформаційної безпеки, а й насамперед співробітники банку, тому крім робіт з поліпшення правової та технічної складової системи безпеки банку не варто забувати про роботу з персоналом, яка включає проведення інструктажів і ретельний контроль за виконанням необхідних правил. Сфера інформаційної безпеки — найбільш динамічна область розвитку індустрії безпеки загалом. Якщо забезпечення фізичної безпеки має давню традицію та усталені підходи, то інформаційна безпека постійно потребує нових рішень, так як комп'ютерні та телекомунікаційні технології постійно оновлюються, і на комп'ютерні системи покладається все більша відповідальність.

Література

1. Банківська безпека: Корченко А.О., Скачек Л.М, Хорошко В.О. За заг. ред. докт. техн. наук, проф. О.В.Хорошка. Київ: ПВП «Задруга», 2014. с.185.

УПРАВЛІННЯ ІНЦИДЕНТАМИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

Бударецький Ю.І., к.т.н., с.н.с.
Львівський національний університет «Львівська політехніка»
м. Львів, Україна
Харитонов О.В., Алексеєнко А.В.
Державний університет телекомунікацій
м. Київ, Україна

Автоматизована система управління (АСУ) [1] – автоматизована система, що ґрунтується на комплексному використанні технічних, математичних, інформаційних та організаційних засобів для управління складними технічними й економічними об'єктами. АСУ призначені для прискорення процесу оброблення інформації і створюються та функціонують у всіх сферах людської діяльності. В епоху інформаційної революції, як і у всіх інформаційних системах, де створюється, поширюється, передається і зберігається інформація з різним ступенем конфіденційності, в АСУ також існують інциденти і загрози, на які необхідно реагувати.

Власники бізнесу постійно шукають способи, щоб забезпечити захист компанії від непередбачених інцидентів безпеки, які можуть спричинити значні збитки. Один із способів зробити це – запровадити процес управління інцидентами.

Управління інцидентами – це процес, який використовується спеціалістами з кібербезпеки, IT-фахівцями для виявлення інцидентів у

організаціях та реагування на них. Інциденти кібербезпеки можуть бути будь-якими: від збою сервера до витоку даних, або чогось такого, як неправильне налаштування брандмауера працівником. Управління інцидентами кібербезпеки має на меті мінімізувати вплив цих інцидентів на бізнес-операції та запобігти їх повторенню [2]. Необхідно усвідомити, що управління інцидентами інформаційної безпеки не запобігає нанесенню збитків, тому що він уже відбувся і збитки нанесені. Функцією системи управління інцидентами є розслідування інциденту і своєчасне впровадження превентивних корегувальних заходів для зниження імовірності його повторення наступних [3].

Для цього команда управління інцидентами має спочатку визначити причину інциденту та вжити заходів для її усунення та переконатися, що використовує всі належні процедури для запобігання повторенню інцидентів.

Команди управління інцидентами використовують кілька інструментів і технологій, щоб допомогти організаціям належним чином реагувати на інциденти. Деякі з найпоширеніших інструментів включають:

- системи виявлення вторгнень (ці системи виявляють і реагують на інциденти безпеки. Вони часто мають такі функції, як сповіщення в реальному часі та звітування);
- аналізатори Netflow [4] (ці інструменти допомагають спеціалістам з управління інцидентами проаналізувати трафік, що надходить у мережу та виходить із неї і ця інформація може ідентифікувати зловмисну активність і швидко реагувати на інциденти);
- сканери вразливостей (ці сканери допомагають виявляти вразливі місця в системах і мережах організації, цю інформацію можна використовувати для усунення вразливостей і запобігання майбутнім інцидентам);
- моніторинг доступності (цей тип моніторингу допомагає спеціалістам з управління інцидентами відстежувати доступність критичних систем і програм, цю інформацію можна використовувати для швидкого виявлення та вирішення інцидентів, що впливають на бізнес-операції);
- веб-проксі – це сервер, розташований між клієнтом і цільовим сервером, який перехоплює всі запити від клієнта та пересилає їх на цільовий сервер (це можна використовувати для моніторингу трафіку та блокування доступу до певних веб-сайтів);
- інструменти безпеки інформації та керування подіями (SIEM), які збирають і аналізують дані безпеки в організації (це може допомогти спеціалістам з управління інцидентами швидко визначити та пом’якшити будь-які потенційні загрози);
- розвідка загроз – це інформація про поточні або нові загрози, які можуть вплинути на організацію (цей інструмент можна використовувати, щоб допомогти командам управління інцидентами, випередити будь-які потенційні атаки та захистити свій бізнес).

Таким чином, внутрішні команди, використовуючи інструменти управління інцидентами можуть допомогти організаціям оперативно реагувати

на будь-які інциденти у їх АСУ та захистити свій бізнес від потенційних атак, наприклад, створивши політику реагування на інциденти для всієї організації.

Література

1. ДСТУ 2941-94. Системи оброблення інформації. Розроблення систем. Терміни та визначення. Видання офіційне. Київ, 1994. 19 с.
2. Про електронні комунікації. Закон України. Редакція від 19.11.2022. URL: https://zakon.rada.gov.ua/laws/show/1089-IX#Text (дата звернення 19.02.2023).
3. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки: навч.посібник. /Корченко О.Г., Центр навч. – наук. та наук.-пр. видань НА СБ України, 2014. 190 с.
4. 15 найкращих інструментів моніторингу мережі, протестовані в 2020 році. URL: https://www.issp.training/post/shcho-take-upravlinnya-intsydentamy-ta-yaki-yoho-perevahy

МОДЕЛЬ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ МАТРИЧНИХ ІГОР

Шиповський В.В.
Національний університет оборони України імені Івана Черняховського
м. Київ, Україна

У 2022 році відбулось широкомасштабне вторгнення в Україну з боку рф, крім військових дій, російські спецпідрозділи провели ряд кібероперацій, намагаючись зламати інформаційні системи об’єктів критичної інфраструктури та веб-ресурсів державних установ. Аналіз активних кібервпливів (КВ) на інформаційні системи об’єктів критичної інфраструктури та веб-ресурси державних установ є надзвичайно важливим для забезпечення кібербезпеки країни. Він дозволяє виявити можливі вразливості та вразити, зміцнити захист систем та убезпечити їх від кібератак. Аналіз активних КВ на інформаційні системи об’єктів критичної інфраструктури та веб-ресурси державних установ в Україні під час російського вторгнення у 2022 році підкреслив важливість кібербезпеки для державної безпеки та стабільності країни. Враховуючи вищезазначене, сьогоденність вимагає постійної підтримки належного рівня кіберстійкості (КС), якій забезпечить відповідний рівень захисту інформаційних систем об’єктів критичної інфраструктури. Для розроблення методики оцінювання КС

Модель оцінювання КС з використанням теорії ігор може бути корисною для оцінки ризиків та визначення стратегій захисту від кібератак. Теорія ігор досліджує взаємодію між гравцями, що мають різні цілі та можливості, та

дозволяє прогнозувати поведінку гравців та визначати оптимальні рішення в умовах невизначеності та ризику[1].

Для розробки моделі оцінювання КС з використанням теорії ігор необхідно визначити гравців, їх цілі та можливості. Наприклад, у кібербезпеці можуть бути два гравці: нападник та захисник. Нападник має ціль зламати систему, отримати доступ до конфіденційної інформації або завдати шкоди, а захисник має ціль захистити систему від таких атак. Умови гри можуть включати різні параметри, такі як технічні характеристики системи, рівень доступності та надійності, можливість виявлення атак та здібності гравців.

Далі можна застосувати методи теорії ігор, такі як матричні ігри, гра з неповною інформацією або гра з повторюваними іграми, щоб розглянути різні сценарії та визначити найоптимальніші стратегії для кожного з гравців. Наприклад, можна досліджувати, як змінюється стратегія нападника в залежності від технічних параметрів системи, чи як змінюється стратегія захисника в залежності від інформації про попередні атаки. Якщо перший гравець має *m* стратегій, а другий гравець — *n* стратегій, то матрична гра може бути задана *m*×*n*-матрицею:

$$A = [aij]m \times n \quad (1)$$

де *aij* — виграш першого гравця, якщо він обрав свою стратегію *i (i = 1, 2, ..., m)*, а другий гравець обрав свою стратегію *j (j = 1, 2, ..., n)*.

При виборі стратегій в матричних іграх гравцям слід користуватись принципом максиміна. Матрична гра завжди має розв'язок в змішаних стратегіях. Елементарною матричною грою є гра з 2×2-матрицею (2×2-гра).

Отже, модель оцінювання КС ІС ОКІ з використанням теорії ігор може допомогти визначити найкращі рішення в умовах невизначеності та ризику, забезпечити ефективний захист системи та зменшити можливі витрати на кібербезпеку.

Однак, при застосуванні теорії ігор для оцінювання КС ІС ОКІ необхідно враховувати деякі обмеження. Наприклад, в реальному світі можуть бути додаткові фактори, які не були враховані у моделі, а також можуть виникнути непередбачувані ситуації, які можуть вплинути на стратегію гравців. Крім того, можуть існувати гравці, які не мають зацікавленості в зламі системи, але все ж можуть використовувати її слабкі місця для отримання користі.

Таким чином, при застосуванні теорії ігор для оцінювання КС ІС ОКІ необхідно розглядати модель як інструмент для планування та прийняття рішень, а не як універсальний метод для вирішення всіх проблем з кібербезпекою. Важливо також враховувати реальні обмеження та фактори, що впливають на систему, а також використовувати інші методи та підходи для забезпечення КС системи.

Література

1. Як росія та Україна воюють на кіберфронті.. URL: http://web.znu.edu.ua/herald/issues/2012/eco-3-2012/059-64.pdf

2. Барановська Л.В. Теорія ігор: курс лекцій. Навчальний посібник. Національний технічний університет України “Київський Політехнічний інститут імені Ігоря Сікорського”. *Електронне мережне навчальне видання.* 2022. С. 31–64.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ ДО ВПРОВАДЖЕННЯ ТА РЕАЛІЗАЦІЇ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВІТЧИЗНЯНИХ ТА ЗАРУБІЖНИХ КОМПАНІЯХ

Ліпатова С. В.
Державний університет телекомунікацій
м.Київ, Україна

Анотація. У зв’язку з стрімким розвитком інформаційних технологій з кожним днем зростає потреба у захисті інформації. Але обробка, передача та захист інформації пов'язані з ризиком, який необхідно враховувати, оцінювати та керувати для успішної роботи організації. В даний час на практиці використовуються різні методи оцінки та управління інформаційними ризиками.

Ключові слова: система захисту інформації, ризик, процес управління.

Ризик інформаційної безпеки – це потенційна можливість використання вразливостей активів конкретною загрозою заподіяння шкоди організації.

Цілі процесу аналізу ризиків ІБ:

1. Ідентифікувати активи та оцінити їх цінність
2. Ідентифікувати загрози активам та вразливості у системі захисту
3. Прорахувати ймовірність реалізації загроз та їх вплив на бізнес
4. Дотриматися балансу між вартістю можливих негативних наслідків та вартістю заходів захисту, дати рекомендації керівництву компанії з обробки виявлених ризиків [1, с. 89].

Розглянемо найвідоміші методики управління ризиками інформаційної безпеки: CRAMM, COBIT for Risk, FRAP, Octave, Microsoft.

CRAMM — це метод аналізу ризиків, розроблений британською урядовою організацією ССТА (Центральне агентство зв'язку та телекомунікацій), яка нині перейменована в Office of Government Commerce (OGC). Інструмент з такою самою назвою підтримує метод CRAMM. Метод CRAMM досить важко використовувати без інструмента CRAMM. Перші випуски CRAMM (метод та інструмент) були засновані на передовому досвіді британських урядових організацій. В даний час CRAMM є кращим методом аналізу ризиків уряду Великобританії, але CRAMM також використовується в багатьох країнах за межами Великобританії. CRAMM особливо підходить для великих організацій, таких як державні органи та промисловість. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу.

Методологія COBIT for Risk. Організації повинні розуміти, що COBIT є наскрізною структурою, яка розглядає оптимізацію ризиків як ключову мету. COBIT розглядає керівництво та управління ризиками як частину загального керівництва та управління корпоративними IT [3, с. 51].

Існує 2 виділені процеси: один в домені управління (оцінка, управління та моніторинг [EDM]), а інший в домені управління (вирівнювання, планування та організація [APO]), які представляють забезпечення оптимізації ризиків (EDM03) та управління ризиками (APO12) відповідно. Управління ризиками вбудоване у структуру COBIT.

Крім цього, COBIT для управління ризиками виділяє ключові допоміжні процеси з структури COBIT для функції управління ризиками. Організації можуть отримувати вихідні дані щодо конкретних ризиків, такі як стратегія управління ризиками, план комунікацій з управління ризиками, а також фінансові та бюджетні вимоги для реагування на ризики та їх зниження. Це також допоможе їм відстежувати показники та цілі ризику та складати звіти про проблеми недотримання та основні причини.

Методика FRAP орієнтована якісну оцінку ризиків ІБ з погляду їхнього впливу досягнення бізнес-цілей організації, а чи не виконання якихось каталогів заходів безпеки чи вимог аудиту. FRAP розшифровується як "Спрощений процес аналізу ризиків". Це формальна методологія, розроблена, щоб бути швидкою та простою. Основні кроки включають [2, с. 109]:

- Мозковий штурм для складання списку загроз,
- Призначення простої ймовірності (тобто високої/середньої/низької) кожній загрозі,
- Присвоєння кожній загрозі простого впливу (тобто високого/середнього/низького),
- Ідентифікація засобів контролю для перелічених загроз та
- Резюме керування.

FRAP дозволяє провести повний аналіз ризиків за кілька годин або днів, надаючи пріоритетний список загроз та засобів контролю. Це дозволяє керівникам швидко приймати рішення щодо затвердження проектів та бюджетів, надає вагомі підстави для впровадження економічно ефективних засобів контролю для обмеження впливу та часто виявляє потреби в ресурсах та навичках.

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) — методика поведінки оцінки ризиків в організації, що розробляється інститутом Software Engineering Institute (SEI) при університеті Карнегі Меллон (Carnegie Mellon University) [5, с. 31].

Підхід Operationally Critical Threat Threat, Asset та Vulnerability EvaluationSM (OCTAVE) визначає метод стратегічної оцінки та планування безпеки на основі ризиків. OCTAVE — це самоврядний підхід, що означає, що люди з організації беруть він відповідальність за розробку стратегії безпеки організації. OCTAVE — це варіант підходу, адаптований до обмежених засобів та унікальних обмежень, які зазвичай зустрічаються в невеликих організаціях

(менше 100 осіб). OCTAVE очолює невелика міждисциплінарна група (від трьох до п'яти осіб) персоналу організації, яка збирає та аналізує інформацію, розробляючи стратегію захисту та плани пом'якшення наслідків на основі унікальних операційних ризиків безпеки організації. Для ефективного проведення OCTAVE команда повинна мати широкі знання бізнес-процесів та процесів безпеки організації, щоб вона могла самостійно виконувати всі дії.

Методика управління ризиками інформаційної безпеки, запропонована корпорацією Microsoft у 2006 році, викладена у її «Посібнику з управління ризиками безпеки». Процес управління ризиками, пропонований корпорацією Microsoft, розбиває етап оцінки ризиків на наступні три кроки [2, с. 108]:

– Планування. Розробка основи для успішної оцінки ризиків.

– Координований збір даних Збір інформації щодо ризиків під час координованих обговорень ризиків.

– Приоритизація ризиків. Ранжування виявлених ризиків на основі несуперечливого та повторюваного процесу.

Для проведення оцінки потрібно зібрати дані про: активи організації, загрози безпеці, уразливості, поточне середовище контролю, пропоновані елементи контролю.

Процес управління ризиками безпеки, який пропонує корпорація Microsoft, визначає такі якісні класи активів: — високий, середній та низький вплив на бізнес.

Для загроз вказується рівень впливу відповідно до концепції багаторівневого захисту (рівні – фізичний, мережі, хоста, додатки, даних).

Вибір методики управління ризиками інформаційної безпеки, що підходить для кожної організації, залежить від низки умов її діяльності [6, с. 4]:

– залежність діяльності організації від інформаційних технологій та значимість для її діяльності ризиків інформаційної безпеки;

– необхідність детального вивчення ризиків інформаційної безпеки та можливість проведення верхньорівневої оцінки ризиків та визначення базових напрямів щодо зниження ризиків інформаційної безпеки;

– наявність людських, фінансових та тимчасових ресурсів для реалізації процесу управління ризиками інформаційної безпеки;

– вимоги законодавства, регуляторів та інших заінтересованих сторін щодо процесу управління ризиками інформаційної безпеки.

Література

1. Гарасим Ю. Р. Аналіз систем захисту інформації. *Військово-технічний збірник*. № 1 (4). 2010. С. 87-95.

2. Гарасим Ю.Р., Ромака В. А., Рибій М. М. Забезпечення неперервності функціонування систем захисту інформації. *Вісник НУ «Львівська політехніка» «Автоматика, вимірювання та керування».* 2012. № 741. С. 105-112.

3. ISO/IEC 27035. Information technology. *Security techniques. Information security incedent management*. 2011. 78 p.

4. Swanson M., Bowen P., Phillips A. W., Gallup D., Lynes D. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems.. 2010. 149 p.
5. Alberts C. J., Behrens S. G., Pethia R. D., Wilson W. R. Operationally Critical Threat, Asset and Vulnerability Evaluation S. G. Behrens, R. D. Pethia, W. R. Wilson. 1999. 84.
6. Гарасим Ю. Р. Аналіз ризиків при забезпеченні неперервності функціонування систем захисту інформації: матеріали Шістнадцятої Всеукраїнської наукової Інтернет-конференції. Тернопіль: Тайп, 2012 С. 3-5.

СУЧАСНІ ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Скрипка О. В.
Державний університет телекомунікацій
м. Київ, Україна

В часи військових дій на території країни питання забезпечення стабільного функціонування усіх державницьких процесів виходить на перший план. За таких умов неабиякої ролі набуває стала робота об’єктів критичної інфраструктури. Саме синергія фізичного та кіберзахисту об’єктів критичної інфраструктури стала головною темою засідання Національного Кластера Кібербезпеки [1]. На відміну від багатьох інших галузей, мережі критичної інфраструктури також використовують інформаційні (IT) та операційні технології (OT). IT-системи включають комп’ютери, сервери та мобільні пристрої, а також інформацію, що передається між ними. В свою чергу, OT включають фізичні пристрої або програмне забезпечення, які контролюють операції в реальному світі: насоси, клапани, лічильники, роботизовану техніку тощо. Компанія Unearth, яка допомагає постачальникам критичної інфраструктури керувати фізичними активами, опублікувала статтю про 5 способів запобігти кібератакам на критичну інфраструктуру [2]. Виділимо основні аспекти :

1. Розвиток культури кібербезпеки. Фішингові, брутфорс атаки та атаки "нульового дня" ставлять під загрозу систему, коли один працівник завантажує файл зі шкідливим програмним забезпеченням або помилково надає свої облікові дані кіберзлочинцю, чи не встановлює патчі оновлень та нехтує надійністю паролів. Більшість зломів відбуваються через недостатню підготовку, відсутність протоколів або людські помилки. Кожен повинен пройти навчання щодо поширених атак та вразливостей, пам’ятати про необхідність оновлення та захисту своїх пристроїв, а також бути обізнаним щодо тенденцій у сфері кіберзлочинності. Компанія Bricata, що спеціалізується на кібербезпеці, рекомендує маркетинговим командам співпрацювати з експертами з кібербезпеки, щоб розвивати культуру кібербезпеки [3] в організації. Крім того,

комунальним підприємствам необхідно розробити ефективні плани реагування на інциденти, обмінюватися кращими практиками у своїй мережі та заохочувати прозорість, повідомляючи про атаки в державні органи. Можна навіть організовувати кібернетичні "військові змагання" між Blue і Red командами [4], щоб перевірити свої протоколи щодо захисту систем.

2. Інвестиції в цифрову та фізичну безпеку. Впровадження найкращих практик та розвиток культури кібербезпеки, звичайно, має свою ціну – але поки хакери шукають вразливості у IT/OT-мережах, також потрібно розширити команду кібербезпеки та інвестувати у фізичну безпеку. Для оновлення мережі важливо залучати молодих спеціалістів. Інвестиції в молоді таланти та збільшення штату також важливі для підвищення рівня кібербезпеки. Багато комунальних підприємств не мають ні талантів, ні чисельності, щоб конкурувати з досвідом кіберзлочинців. Найм команди або принаймні однієї талановитої людини, яка зосередиться виключно на кібербезпеці, є важливим кроком у правильному напрямку. В умовах конвергенції OT та IT не можна нехтувати фізичною безпекою. Є багато об'єктів, що обслуговують клієнтів, таких як зарядні станції або "розумні" лічильники, які необхідно захистити, щоб запобігти будь-якому втручанню або доступу до мережі. Оскільки комунальні підприємства мають широке поле для атак, і кіберзлочинці будуть використовувати будь-яку слабкість, необхідно посилити захист як цифрових, так і фізичних активів.

3. Сприяння чіткій комунікації та лідерства. Часто кібервразливості виникають через брак комунікації та лідерства, особливо актуально для постачальників критичної інфраструктури. В компаніях, часто виникають інформаційні ізолятори – відсутність комунікації та співпраці між командами. Потрібно забезпечити наявність централізованої команди з кібербезпеки та надати їй повноваження приймати відповідні рішення. Також необхідно створити протоколи, яких всі будуть дотримуватися, узгоджені в операційних та IT-мережах. Крім того, для цих цілей виділяється відповідний бюджет. Регулярне інформування керівництва, ради директорів та менеджерів щодо тенденцій, вразливостей та пріоритетів є необхідною умовою для розвитку у сфері кібербезпеки.

4. Впровадження найкращих практик кібергігієни. На Рис. 1 зображено перелік найпоширеніших засобів захисту.

Також можна найняти компанію або консультанта з кібербезпеки. Все частіше для моніторингу мереж використовуються Big Data та штучний інтелект. Якщо найкращі практики вже впроваджені, почніть реалізовувати послідовну стратегію нульової довіри [5], яка передбачає, що компанію зламали і дозволить пом'якшити внутрішні загрози.

5. Аудит пристроїв, активів та інших компонентів мережі

Не можна захистити те, про що ніхто не знає, тому важливо проводити аудит усіх пристроїв у мережі таких як особисті пристрої (Bring Your Own Device), мережі і сайти, сторонні сервіси, мобільні пристрої, розумні технології та IoT (Інтернет речей), інше різноманітне програмне та апаратне забезпечення.

Рис. 1. Найпоширеніші засоби захисту

Повна прозорість організації та поглиблений аудит фізичних та цифрових активів є необхідними. Ретельно перевіряйте вразливості вашої організації до того, як це зробить кіберзлочинець. Оскільки питання щодо безперервності критичної інфраструктури стають все більше актуальнішими, кібербезпека повинна бути на першому плані і в центрі уваги. Хоча кібербезпека може вимагати значних змін у культурі та ресурсах, атаки на критичну інфраструктуру неминучі і комунальні підприємства можуть та повинні знайти рішення.

Література

1. Засідання Національного Кластера Кібербезпеки. URL: https://cybersecuritycluster.org.ua/news/bezpeka-krytychnoyi-infrastruktury-u-fizychnomu-ta-kiberprostori-rezultaty-zasidannya-naczionalnogo-klastera-kiberbezpeky/
2. Стаття Unearth про 5 способів запобігти кібератакам на критичну інфраструктуру. URL: https://www.unearthlabs.com/blogs/cybersecurity-critical-infrastructure
3. Рекомендації Bricata щодо культури кібербезпеки. URL: https://blogs.opentext.com/category/technologies/security/
4. Coursera: Red Team vs. Blue Team in Cybersecurity. URL: https://www.coursera.org/articles/red-team-vs-blue-team

5. Що таке Zero Trust? Модель безпеки. URL: https://blog.1gb.ua/perevod-chto-takoe-zero-trust-model-bezopasnosty/

METHODS OF DETECTION AND ANALYSIS OF MALICIOUS SOFTWARE

Y. Pepa, PhD, M. Yurchenko
State University of Telecommunications
Kyiv, Ukraine
I. Mykhalchuk, PhD
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

It is well known that there is malicious software (malware), which is intended for unauthorized interference with the operation of automated systems (AS) or computer networks of state infrastructure facilities [1]. This leads to information leakage, loss, falsification, destruction or blocking of the entire automated system. There are three main ways to search for an malware.

The first method is based on the use of antivirus programs to scan storage media that may potentially contain malware. The advantages of this method are simplicity and speed. At the same time, the disadvantage of this method is that the antivirus may not detect the malicious program. The reason for this is that a certain period of time passes between the appearance of the malware and the entry of its signature into the antivirus signature database. In addition, it should be borne in mind that different antiviruses have slightly different algorithms, and different antivirus laboratories have different criteria for classifying programs as malware. It should also not be ruled out that a certain malicious program developed by the special services of a foreign country may deliberately not be detected by an antivirus developed in the same country. In view of the above, it is advisable to use several anti-viruses (at least two or three) to search for malware, and it is desirable that at least one of them is of domestic development, and the foreign ones are from different countries of origin.

The second method is to isolate (sift out) files that are known to be useful. Its essence is as follows. Having the checksums (hashes) of files of useful programs, such as operating systems, office applications, graphic editors, etc., the expert can exclude these files from the search area. The hashes of useful files can be obtained, for example, from the NSRL [2]. A similar method is used to search for malware in RAM (RAM dump) – knowing the normal configuration of processes in memory, you can identify atypical ones that should be investigated more thoroughly.

The third way is to start a potentially infected AS and monitor abnormal activity (for example, opening "extra" network connections, auto-launching unknown programs, etc.). During such a launch, it is recommended to replace the storage media of the AS with their clones or make bitwise copies of these media in advance to restore their initial state after the examination. It is also possible to run the above bitwise copies

on a virtual machine instead of a real AS. The disadvantage of this method is that abnormal activity may not appear during such a test run because it is scheduled for a different time or configured for other conditions.

You should also pay attention to "duplicate files", i.e. files with the same name but different extensions (for example, *.com and *.exe). This is the method used by satellite viruses.

In addition, it should be remembered that the malware can change the environment variables of the Windows operating system. For example, the path to the folder with the malware files can be added to the system variable PATH (indicating the search paths for executable files). If this new path is specified at the beginning of the path list, executable files will be searched in this new, "malicious" folder first. It is also possible to modify the system variable PATHEXT (containing a list of extensions recognized by the operating system as executable file extensions) by adding a new extension to the top of the list. Taking into account that executable files with the same name are executed in the order of their extensions in the specified variable, after the specified manipulations, files with the new, "malicious" extension will be executed first.

So, to be on the safe side, it is recommended to check all these variables.

References

1. Cyber-Attack Against Ukrainian Critical Infrastructure. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

2. National Software Reference Library. URL: https://www.nist.gov/itl/ssd/software-quality-group/nsrl-download

METHODS OF RESEARCH OF MALICIOUS SOFTWARE

Y. Pepa, PhD, O. Panasiuk, I. Krotov
State University of Telecommunications
Kyiv, Ukraine

During the investigation of cyber incidents, important information can be obtained from the attacked automated system or from the attacker's computer, as well as from intermediate network nodes [1]. There are two ways to study the behavior of an malware: static and dynamic research.

Static analysis involves examining the program code without running it. There are basic and advanced static analysis.

Basic static analysis involves examining the structure of a suspicious file, the types of related functions and dynamic libraries, the type of compiler and packer of the file, and searching for text strings that may be contained:

- URLs accessed by the program tool;
- IP addresses accessed by the software tool;
- memory addresses;

- instructions of the central processor;
- data used by the program.

Extended static analysis involves disassembling the program code and further examining the resulting disassembled code to find certain instructions, system calls, etc. that provide the functionality of the file under investigation.

Dynamic testing involves running the program under investigation in a controlled environment and recording all its actions. By analogy with static analysis, there are basic and advanced dynamic analysis.

In basic dynamic testing, the program is run in a controlled environment, which can be either virtual (virtual machine, sandbox) or real (test computer). Monitoring utilities record all actions of the program under investigation: creating/deleting files and folders, changing their parameters (such as "invisible", "system", "read-only", etc.), modifying entries in the operating environment settings files (MS Windows registry, corresponding Unix/Linux settings files of similar operating systems), opening network connections and transferring information, etc. In particular, the basic dynamic analysis detects process substitution by verifying signatures and/or comparing strings in the file properties on disk and in memory. To detect malicious libraries (DLLs), you can use Dependency Walker (included in the Process Explorer software).

It should be noted that to examine malicious documents (infected PDF files, etc.), you should use unpatched and unhacked viewers.

To detect changes in the registry, you can compare the registry before and after the malware launch. For this purpose, you can use Regshot software. The Process Monitor software also tracks changes to the registry, recording which process makes these changes.

To intercept network requests, it is advisable to use a network simulation (the so-called fake network, which can be implemented, for example, with INetSim software that simulates Internet services), as well as software for intercepting network messages (sniffers): NetCat, WireShark, tcpdump, Process Monitor. To intercept DNS queries, you can use ApateDNS software, which simulates the operation of a DNS server and intercepts/fixes DNS queries). You should also check which ports are opened for listening on the affected computer (malware often opens non-standard ports: for example, an SSL port is opened by another service or vice versa).

It should be noted that certain types of malwares have protection mechanisms that allow the malicious program to "understand" that it is running in a sandbox or virtual machine and, accordingly, not activate its functions.

Advanced dynamic investigation involves studying the functionality of a program with the help of a debugger or debugger, i.e., a computer program used to test and fix flaws in other programs. A debugger allows you to run the disassembled code of a program and track the process of this program's functioning step by step.

It should be noted that for reliable protection of the computer and data [2], it is worth performing an additional check, i.e., running the malware through one or more anti-virus programs in dynamic mode, as well as heuristically.

References

1. Samoilenko O.A. Basic Methods of Investigating Crimes Committed in Cyberspace: Monograph / O.A. Samoilenko. – Odesa: TES, 2020. – 372 p.
2. Prevention of Cybercrime. URL: http://www3.weforum.org/docs/ WEF_Cybercrime_Prevention_ISP_/Principles.pdf

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ БАНКІВСЬКИХ ТРАНЗАКЦІЙ В СИСТЕМАХ ІНТЕРНЕТ-БАНКІНГУ

Брус Б.Ю.
Державний університет телекомунікацій
м. Київ, Україна

Сучасні технології дозволяють здійснювати банківські операції через інтернет-банкінг, що є зручним та швидким способом управління фінансами. Однак, разом з цим зростає і ризик шахрайства та крадіжки коштів через комп'ютерні вторгнення та інші шахрайські дії. У зв'язку з цим, виникає потреба в підвищенні ефективності захисту банківських транзакцій в системах інтернет-банкінгу.

Для підвищення захисту банківських транзакцій в інтернет-банкінгу можна використовувати наступні методи:

1. Двофакторна аутентифікація - цей метод полягає у використанні двох різних механізмів для підтвердження ідентичності користувача. Наприклад, це може бути поєднання пароля та коду, що надсилається на мобільний телефон користувача.
2. Використання SSL-шифрування - SSL-шифрування дозволяє забезпечити безпеку обміну даними між сервером та клієнтом. Шифрування забезпечує те, що дані, що передаються між сервером та клієнтом, не можуть бути перехоплені третіми особами.
3. Використання систем детекції вторгнень (IDS) та систем захисту від вторгнень (IPS) - ці системи дозволяють виявляти та блокувати вторгнення на різних етапах банківських транзакцій. IDS дозволяє виявити вторгнення та повідомити про це відповідальну службу, а IPS може блокувати зловмисний трафік.
4. Використання захищених каналів зв'язку – захищені канали зв'язку дозволяють забезпечити захищений обмін даними між банківським сервером та клієнтом. Це забезпечується за допомогою протоколів шифрування, таких як TLS або SSL. Використання захищених каналів зв'язку знижує ризик перехоплення та зловживання даними клієнтів.
5. Моніторинг активності користувачів - відстеження активності користувачів у системі інтернет-банкінгу може допомогти виявити незвичайну або підозрілу поведінку, що може свідчити про спробу шахрайства.
6. Підвищення рівня освіти користувачів - користувачі систем інтернет-

банкінгу повинні бути розуміти ризики та методи захисту своїх фінансів. Вони повинні бути проінформовані про те, як використовувати систему безпечно та про те, які дії необхідно здійснювати у випадку підозрілого поведінки.

Для досягнення максимальної ефективності захисту банківських транзакцій в системах інтернет-банкінгу необхідно використовувати комплексний підхід, що включає в себе використання кількох методів захисту одночасно. Також важливо регулярно оновлювати програмне забезпечення та вчасно виявляти та ліквідовувати можливі уразливості систем.

Література

1. Internet banking safety tips: 8 tips to use internet banking safely. *The Economic Times*. URL: https://economictimes.indiatimes.com/wealth/spend/8-tips-to-use-internet-banking-safely/articleshow/55113849.cms.
2. The top 10 cybersecurity threats to digital banking and how to guard against them - guardrails. *GuardRails*. URL: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/.

СЕКЦІЯ 7. ОСВІТА Й ОБІЗНАНІСТЬ, ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА. ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ

Сичевський А.С
Державний університет телекомунікацій
м.Київ, Україна

Загрози соціальної інженерії є одними з найскладніших ризиків, від яких потрібно захиститися в корпоративному середовищі безпеки.

Соціальна інженерія – це тип атаки, націленої на людей шляхом маніпулювання ними для надання конфіденційної інформації, таких як паролів і бізнес-даних. Цей тип атаки є високоефективним і може завдати серйозної шкоди інформаційній безпеці підприємства.

Для ефективного захисту від атак соціальної інженерії підприємство має запровадити комплексний план безпеки, який передбачає навчання та навчання працівників, технічні заходи протидії та процедури реагування на інциденти.

Програми навчання та навчання працівників повинні бути розроблені для підвищення обізнаності про типи атак соціальної інженерії та про те, як їх ідентифікувати та реагувати на них.

Для захисту від атак соціальної інженерії план має включати низку тем, таких як:

- - тренінги з розпізнавання потенційних атак соціальної інженерії,
- розуміння того, як зловмисники використовують методи соціальної інженерії,
- розробка політик безпеки та процедур для ваших співробітників, навчання персоналу безпечним методам використання в Інтернеті та надання інформації про ризики, пов'язані з обміном конфіденційною інформацією.

Крім того, співробітникам слід нагадати про важливість захисту своїх облікових записів і паролів в Інтернеті.

Нарешті, дуже важливо проводити постійні оцінки вашої політики навчання та безпеки, щоб переконатися, що вони актуальні та ефективні.

Технічні заходи протидії, які можуть допомогти зменшити ризик атаки соціальної інженерії, включають двофакторну автентифікацію, шифрування та класифікацію даних.

Нарешті, підприємства повинні мати чіткі процедури реагування на інциденти безпеки, включаючи протоколи ескалації, групи реагування на інциденти та процедури звітування про інциденти.

Приклад процедури реагування на інцедент, що пов'язані з соціальною інженерією:

- Інциденти, пов'язані з соціальною інженерією, передбачають спочатку ідентифікацію та оцінку загрози. Це має включати збір якомога більшої кількості інформації, наприклад, хто був зловмисником, які методи він використовував, які системи постраждали та скільки даних було зламано.
- Потім системи слід негайно ізолювати від решти мережі, щоб запобігти подальшому пошкодженню.
- Після ізоляції систем слід провести ретельне розслідування інциденту та вжити необхідних заходів для зменшення ризику, наприклад запровадити додаткові протоколи безпеки або оновити існуючі.
- Нарешті, будь-які необхідні повідомлення слід надсилати регуляторним і правоохоронним органам, а також іншим зацікавленим сторонам.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021.
URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 14.03.2023).

ПОБУДОВА ЕФЕКТИВНОГО ПРОЦЕСУ ПІДВИЩЕННЯ КІБЕРНЕТИЧНОЇ ОБІЗНАНОСТІ ПРАЦІВНИКІВ

Курбет Д.Г.
Державний університет телекомунікацій
м. Київ, Україна

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу.

Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони.

Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 року № 2824-IV, а також відповідні закони України та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України. Важливий практичний крок у реалізації наявної нормативно-правової бази було зроблено створенням 2007 року Центру реагування на комп'ютерні інциденти, що ввійшов до складу Державної служби спеціального зв'язку та захисту інформації України. На виконання статті 35 згаданої Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки (СБ) України на базі спеціального підрозділу для боротьби з кіберзагрозами запрацював Національний контактний пункт формату 24/7 із реагування та обміну терміновою інформацією про вчинені кіберзлочини.

Окрім того, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року № 34 у структурі СБ України створено 5 Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ — Департамент боротьби з кіберзлочинністю та торгівлею людьми.

Такий стан справ фактично означає, що Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче. Одна з головних причин цих негараздів полягає в «незадовільному кадровому забезпеченні відомств відповідними фахівцями у сфері інформаційної безпеки», як наголошується в аналітичній доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України». Отже, найбільшу загрозу вітчизняним установам і відомствам становить відчутна нестача професіоналів з інформаційної та кібербезпеки, здатних:

- відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу;

- виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки;

- протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.

Дедалі вища активність так званого когнітивного базису — звичайних користувачів, професійних шпигунів і/або хакерів (порушників), поряд зі стрімко зростаючою кількістю способів і методів, до яких вони вдаються з метою пошуку й збору інформації з відкритих і відносно відкритих джерел та її добування із закритих електронних джерел, потужний сплеск розвитку соціальних мереж — це ті чинники, що активізують кіберзлочинність, особливо з огляду на тенденції розвитку інтернету в напрямку інтеграції та об'єднання наявних можливостей у рамках єдиних багатокористувальницьких веб-платформ.

Саме тому глобальна мережа перетворюється на засіб організації різного роду кібернетичних і соціотехнічних атак, несанкціонованого доступу (НСД) до чужих сайтів, створення сайтів-двійників тощо. Останнім часом такі дії неухильно виходять за межі окремих країн, випереджаючи за темпами зростання всі інші види організованої злочинності.

Література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / ред. В. Б. Толубко. Київ : ДУТ, 2015. 288 с. URL: https://dut.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 13.03.2023).

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ РОЗПІЗНАВАННЯ ФЕЙКІВ У КІБЕРПРОСТОРІ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ З ТОЧКИ ЗОРУ КІБЕРБЕЗПЕКИ

Тищенко В.С.
Державний університет телекомунікацій
м. Київ, Україна

В останні роки кількість фейків у кіберпросторі значно збільшилася. Це стало проблемою для багатьох галузей, включаючи політику, медіа та діловий світ. Недостатньо точна інформація може привести до неправильних рішень, що може впливати на багато людей. Використання інструментів нейронної мережі для розпізнавання фейків стає все більш актуальною темою в кібербезпеці.

Нейронні мережі є потужними інструментами для розпізнавання фейків. Вони здатні зіставляти велику кількість даних та знаходити закономірності між

ними. Для розпізнавання фейків, нейронні мережі можуть бути навчені на основі великої кількості прикладів правдивої та фальшивої інформації. Навчання може включати розпізнавання ознак, що вказують на фальшиву інформацію, такі як спотворення зображення або розбіжності в тексті [1].

Однак, інструменти нейронної мережі для розпізнавання фейків мають свої обмеження. Перш за все, вони можуть бути вразливі до атак, які можуть намагатися змінити приклади, на яких мережа була навчена, або вводити шум в дані, що призводить до неправильних результатів. Крім того, розпізнавання фейків у реальному часі може бути складним завданням, оскільки це вимагає високої швидкодії мережі, що може бути складно досягнути з точки зору обчислювальних ресурсів.

З точки зору кібербезпеки, використання інструментів нейронної мережі для розпізнавання фейків може допомогти виявляти фальшиву інформацію та запобігати поширенню неправдивих заяв. Це може бути корисним для більшості галузей, включаючи політику, медіа, електронну комерцію, тощо. Інструменти нейронної мережі для розпізнавання фейків можуть допомогти забезпечити вищу якість інформації в мережі, що може позитивно впливати на взаємодію між людьми та діяльність бізнесу.

Однак, використання інструментів нейронної мережі для розпізнавання фейків повинно бути доповнене іншими методами, такими як аналіз даних та перевірка відправника. Важливо розуміти, що нейронні мережі не можуть вирішити всі проблеми кібербезпеки, але можуть бути корисним інструментом для зменшення ризику впливу фейків у кіберпросторі.

Також важливо забезпечувати надійну безпеку для інструментів нейронної мережі, які використовуються для розпізнавання фейків. Це може включати захист від атак, обмеження доступу до даних, які використовуються для навчання мережі, а також перевірку відповідності правилам безпеки при розгортанні мережі [2].

Існує безліч інструментів нейронних мереж, які використовуються для виявлення фейків в різних типах медіа. Ось кілька прикладів:

1. GPT-2 і GPT-3 - це глибокі нейронні мережі, які можуть генерувати текст з вражаючою точністю та здатністю імітувати людський стиль. Однак, їх можна використовувати для генерації фейкових новин, коментарів, інтерв'ю, тощо. Інструменти, які використовують нейронні мережі, такі як OpenAI's GPT-3 Detector або Grover, можуть розпізнати ці фейки.
2. DeepFakes - це відео, створене з використанням глибоких нейронних мереж, яке може імітувати живу людину. Ці відео можуть бути використані для створення фальшивих новин, реклами, порнографії, тощо. Інструменти, такі як DeepFaceLab або DeepFake Detection, можуть виявляти такі відео та робити їх непридатними.
3. Фальшиві зображення - це зображення, які були змінені за допомогою фотошопу або інших програм з обробки зображень, щоб змінити їх зміст. Інструменти, які використовують нейронні мережі, такі як Adobe's Content

Authenticity Initiative або Google's Fact Check Explorer, можуть допомогти виявити такі фальшиві зображення.

Ці інструменти використовують навчання з вчителем, щоб навчити нейронну мережу розрізняти фальшиві від справжніх медіа-файлів. Однак, важливо пам'ятати, що нейронні мережі можуть бути обмануті та не завжди можуть бути 100% надійними. Тому, використання таких інструментів повинно бути обережним та здійснюватися з додатковими перевірками та контролем.

Наприклад, нейронні мережі можуть бути підвищеною шкідливою дією, якщо їх навчати на неправильних або нестабільних даних. Це може привести до виявлення фальшивих повідомлень як справжніх або, навпаки, не виявлення дійсних фейків.

Крім того, нейронні мережі можуть бути обмануті шляхом додавання шуму або зміни параметрів медіа-файлів. Це може призвести до того, що навчена мережа вважатиме фальшивий медіа-файл за справжній.

Отже, використання інструментів нейронної мережі для розпізнавання фейків у кіберпросторі має можливості та обмеження з точки зору кібербезпеки. Ці інструменти можуть допомогти забезпечити вищу якість інформації в мережі та запобігти поширенню фальшивої інформації, але вони повинні бути доповнені іншими методами, а також забезпечувати надійну безпеку, щоб уникнути можливих наслідків, пов'язаних з ненадійністю таких інструментів. Для досягнення цієї мети, потрібно постійно вдосконалювати технології розпізнавання фейків та забезпечувати стійку безпеку нейронних мереж, що використовуються в таких цілях.

Одним з можливих варіантів для підвищення якості розпізнавання фейків у кіберпросторі може бути поєднання нейронної мережі з іншими алгоритмами машинного навчання. Наприклад, можна використовувати різні підходи до розпізнавання зображень, залежно від типу фейку, що необхідно виявити. Також, можна використовувати методи аналізу тексту та мовлення, щоб виявляти неправдиву інформацію в текстових повідомленнях та соціальних мережах.

Варто зазначити, що нейронні мережі не завжди можуть бути достатньо точними в розпізнаванні фейків, оскільки поняття фейку може бути різним в залежності від контексту та від мети, на яку спрямований фейк. Тому, використовуючи інструменти нейронної мережі для розпізнавання фейків, важливо бути обережним і здійснювати валідацію результатів з допомогою додаткових методів [3].

Окрім того, що використання інструментів нейронної мережі для розпізнавання фейків є важливим кроком у забезпеченні безпеки в кіберпросторі, воно також є викликом для нашого розуміння того, як ми розуміємо інформацію та її передачу в мережі. Здійснення розумного використання цих інструментів може допомогти забезпечити стійку безпеку наших систем та інформації.

Загалом, використання нейронних мереж для розпізнавання фейків у кіберпросторі відкриває нові можливості для боротьби з дезінформацією та забезпечення безпеки в інтернеті. Однак, використання цих інструментів

повинно бути обережним і здійснюватися з допомогою додаткових методів валідації результатів для забезпечення надійної безпеки.

Література

1. Fake detect: a deep learning ensemble model for fake news detection / N. Aslam та ін. *Complexity*. 2021. Т. 2021. С. 1–8.
URL: https://doi.org/10.1155/2021/5557784
2. Fighting fake news: image splice detection via learned self-consistency / M. Huh та ін. *Computer vision – ECCV 2018*. Cham, 2018. С. 106–124.
URL: https://doi.org/10.1007/978-3-030-01252-6_7
3. Kaliyar R. K., Goswami A., Narang P. Multiclass fake news detection using ensemble machine learning. *2019 IEEE 9th international conference on advanced computing (IACC)*, Tiruchirappalli, India, 13–14 December 2019. 2019.
URL: https://doi.org/10.1109/iacc48062.2019.8971579

ЗАКОНОДАВЧІ РАМКИ ЄС ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРГРАМОТНОСТІ ТА ЦИФРОВОЇ ІНКЛЮЗІЇ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ

Кожина А. В. д.н. держ. упр., доц.
Національний авіаційний університет
м. Київ, Україна

Вибравши європейський напрям Україна відкрила перед собою нові горизонти для розвитку, оскільки в цифрову епоху успішність країни залежить напряму від прогресу в побудові суспільства знань, а цифровий розвиток відіграє ключову роль у прискоренні економічного і соціального розвитку країни в цілому. Агресія Росії проти України посилила необхідність захисту також і кіберпростору через значне посилення кібернападів на державні та приватні цифрові ресурси та сервіси.

Діалог Україна-ЄС у сфері цифрової трансформації є одним з найбільш важливих пріоритетів євроінтеграційних процесів Україна-ЄС, в рамках якого була узгоджена дорожня карта інтеграції України до Єдиного цифрового ринку ЄС та програм: «Цифрова Європа» (Digital Europe), «Цифрове підключення Європи» («Connecting Europe Facility Digital»).

Серед пріоритетних програм цифрового розвитку ЄС на поточний період: Цифровий порядок денний для Європи (Digital agenda for Europe), Цифрове підключення Європи (Connecting Europe Facility Digital), Стратегія Єдиного цифрового ринку (Digital Single Market Strategy for Europe), Підключення до Європейського Гігабітного суспільства (Connectivity for a European Gigabit Society), Програма розвитку загальноєвропейських стандартів у сфері телекомунікацій та цифрових технологій, План дій з цифрової освіти (Digital Education Action Plan (2021-2027)) тощо.

Цифровий порядок денний для Європи (Digital agenda for Europe), ухвалений в рамках стратегії «Європа 2020» («Europe 2020») як одна з її семи ініціатив (flagship initiatives). Документ був ініційований у 2010 р. та передбачає комплекс заходів з метою досягнення амбітних цілей послідовно по етапах до 2020 р. та 2030 р. Його важливою складовою є створення Єдиного цифрового ринку (ЄЦР) [1].

«Цифровий порядок денний для Європи» спрямований на забезпечення глобальної конкурентоспроможності ЄС через розвиток та імплементацію ІКТ та запровадження цифрових технологій в усіх сферах і прошарках соціуму. Це основний діючий проектний документ з розвитку інформаційної сфери ЄС, в якому визначений 101 захід в межах "семи стовпів" (seven pillars) для піднесення економіки ЄС на основі максимальної користі цифрових технологій для громадян і бізнесу [1].

Серед пріоритетів розвитку – розробка панєвропейської стратегії з кібернетичної безпеки («Cyberspace Policy») та спеціальної програми з розвитку індустрії хмарних обчислень та охоплення всієї території ЄС високошвидкісними та ультра-швидкісними широкосмуговими мережами («Connecting Europe Facility»), для чого створюються численні інвестиційні фонди і налагоджується широке приватно-державне партнерство.

У процесі імплементації заявлених в рамках стратегії «Цифровий порядок денний для Європи» локальних підпрограм реалізуються спеціалізовані проекти та ініціативи прикладного рівня, наприклад, проект «Європейське хмарне партнерство» («European Cloud Partnership»).

Ключовими заходами програми на першому етапі до 2020 року були: створення єдиного цифрового ринку, досягнення інтероперабельності (експлуатаційної сумісності) програмного забезпечення і контенту, оптимізація відповідних стандартів, підвищення довіри і безпеки користувачів, розвиток швидкісного інтернету, розвиток наукових досліджень та інновацій, поширення цифрової грамотності і навичок роботи з IT, IT для вирішення соціальних проблем [1].

Європейський цифровий порядок денний на період 2020-2030 рр. зосереджений на створенні безпечних цифрових просторів і послуг, створенні рівних умов для цифрових ринків із великими платформами та зміцненні цифрового суверенітету Європи, одночасно сприяючи досягненню кліматичної нейтральності до 2050 р. Цей етап порядку денного ґрунтується на двох стратегічних ініціативах: «Формування цифрового майбутнього Європи» та «Цифрового десятиліття Європи» (Europe's digital decade).

Серед пріоритетів програми до 2030 року: розвиток квантових обчислень, стратегії блокчейну та торговельної політики на основі блокчейну, орієнтованого на людину, надійний штучний інтелект (AI), напівпровідники, цифровий суверенітет, кібербезпека, гігабітне підключення, 5G і 6G, європейські простори даних та інфраструктура, а також встановлення глобальних технологічних стандартів.

Програма ЄС «Цифрова Європа» (Digital Europe) визначає вирішальну роль цифрових технологій та інфраструктури у приватному житті та бізнес-середовищі та орієнтується на п’ять основних напрямів: суперкомп’ютери, штучний інтелект, кібербезпека, передові цифрові навички та забезпечення широкого використання цифрових технологій в економіці та суспільстві. Ця програма особливо спрямована на переваги для всіх, зокрема на цифрове залучення та стійкість, які є важливими для того, щоб кожен міг зробити свій внесок у цифровий світ і отримати від нього користь. Це доступність цифрових послуг, онлайн-навчання для розвитку навичок і нових знань для покращення професійних можливостей, кар’єрного зростання та самозайнятості та покращення якості життя всіх громадян [2].

Важливими для підвищення кіберграмотності є освітні ініціативи ЄС, зокрема, Плани дій з цифрової освіти. Перший «План дій з цифрової освіти на 2018-2020 роки» визначав 11 дій, метою яких була допомога державам-членам у вирішенні викликів та можливостей, що випливають із використання цифрових технологій в освіті та навчанні.

План дій з цифрової освіти (Digital Education Action Plan (2021-2027)) – це оновлена політична ініціатива ЄС для підтримки сталої та ефективної адаптації систем освіти та навчання держав-членів ЄС до епохи цифрових технологій; він сприяє досягненню цілей Європейської програми навичок, Європейського плану дій із стовпа соціальних прав та «Цифрового компасу 2030: європейський шлях для Цифрового десятиліття». Важливими засадами програми є довгострокове стратегічне бачення високоякісної, інклюзивної та доступної європейської цифрової освіти; а також підтримку цифрових методів навчання та освіти та забезпечення інфраструктури, необхідної для інклюзивного та стійкого дистанційного навчання [3].

Важливою ініціативою ЄС щодо України є програма «EU4Digital: підтримка цифрової економіки та суспільства у Східному партнерстві», яка націлена на розширення переваг Єдиного цифрового ринку ЄС для України з метою стимулювання економічного росту, створення робочих місць, покращення життя людей та допомоги бізнесу. Також започаткований проект «Цифрова трансформація для України» (DT4UA), який триватиме з листопада 2022 року до квітня 2025 року і побудований на досягненнях проектів EGOV4UKRAINE та EU4DigitalUA. Метою проекту є підвищення ефективності та безпеки надання державних послуг та доступу до них для громадян і бізнесу в Україні відповідно до вимог ЄС, а також забезпечити швидке реагування на потреби, викликані війною.

Література

1. Digital Agenda for Europe. URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe (accessed 18.02.2023).
2. The Digital Europe Programme. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme (accessed 18.02.2023).

3. Digital Education Action Plan. URL: https://education.ec.europa.eu/focus-topics/digital-education/action-plan (accessed 18.02.2023).

ІНФОРМУВАННЯ Й НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З УРАХУВАННЯМ ВИДІВ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Примаченко Д.В.
Державний університет телекомунікацій
м. Київ, Україна

Сучасні умови господарювання супроводжуються процесами цифровізації всіх без винятку ділянок діяльності підприємств. Поряд із безумовним позитивним ефектом від активного впровадження цифровізації в діяльність господарюючих суб'єктів, виникають й певні ризики, пов'язані із необхідністю забезпечення належного стану інформаційної безпеки на підприємстві. Важливу роль у забезпеченні інформаційної безпеки відіграє процес інформування й навчання персоналу, оскільки знання потенційних загроз, причин та умов скоєння таких злочинів дозволить працівникам підрозділів служб безпеки підприємств у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зловмисних замахів на інформаційні ресурси та потоки господарюючого суб'єкта.

В умовах сьогодення інформаційні загрози набувають обертів, а через постійну модернізацію потенційно небезпечних з інформаційної точки зору об'єктів, існує постійна потреба в оновленні методів запобігання і протидії загрозам інформаційної безпеки.

З огляду на це, на нашу думку, підґрунтям для вибору підходів до інформування й навчання персоналу у сфері інформаційної безпеки мають бути саме інформаційні загрози, з якими стикаються або потенційно можуть мати справу окремі категорії працівників.

Встановлено, що загрози інформаційній безпеці поділяють на активні та пасивні. Активні загрози інформаційній безпеці спрямовані на порушення функціонування діючої ІС шляхом цілеспрямованої атаки на окремі її компоненти, наприклад потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем.

Пасивні загрози передбачають незаконне використання інформаційних ресурсів і не спрямовані на порушення функціонування певної ІС. До пасивних загроз інформаційній безпеці можна віднести, наприклад, незаконний доступ до окремих баз даних або використання методів прослуховування каналів передачі інформації [1].

З урахуванням поділу загроз на активні й пасивні можна запропонувати такі рекомендації щодо інформування й навчання персоналу у сфері інформаційної безпеки.

1. Процес навчання доцільно поділити на два блоки в залежності від групи загроз інформаційній безпеці: блок протидії активним загрозам і блок протидії пасивним загрозам. Перший блок навчання потрібно спрямувати на оволодіння методами протидії незаконному використанню інформаційних ресурсів і порушенню функціонування певної ІС підприємства, другий блок - на екстрене навчання протидії в разі прямої атаки на ІС підприємства;

2. Забезпечити прикладні аспекти навчання персоналу у сфері інформаційної безпеки шляхом залучення фахівців-практиків із захисту інформації, які показують, як забезпечується безперебійне функціонування засобів програмного захисту інформації підприємства, налагоджується та підтримується робота апаратної частини.

3. Пройти тест на проникнення, а точніше зімітувати реальну атаку, мета якої - знайти можливість отримання доступу до цінних активів компанії та/або людини. Відмінності тесту на проникнення від реальної хакерської атаки полягають в його обмеженнях. Для компенсації обмежень білі хакери отримують деяке послаблення, порівняно з чорними.

Таким чином, для успішного навчання й інформування персоналу з питань інформаційної безпеки з урахуванням видів інформаційних загроз необхідно диференціювати навчання з метою оволодіння методами протидії активним і пасивним загрозам, залучати до навчання практиків з інформаційної безпеки, використовувати методи імітації реальних загроз.

Література

1. Utenkova K. Destabilizing factors of the external and internal environment of enterprise and their effect on economic security. *Ekonomika ta derzhava*. 2019. № 8. С. 44. URL: https://doi.org/10.32702/2306-6806.2019.8.44 (дата звернення: 30.03.2023).
2. Нікіпєлова Є. М. Сутність поняття “безпека” та його використання у системі державного управління й міжнародних відносин. *Міжнародний науковий журнал «Інтернаука»*. 2018. Т. 1, № 10. С. 29–35.
3. Горбатюк С. Є. Еволюція феномену безпеки: від стародавніх політико-правових учень – до сучасної наукової думки. *Вісник НАДУ при Президентові України*. 2016. № 2. С. 28–35.

ПРОБЛЕМАТИКА ЗАХИЩЕНОСТІ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД СОЦІОІНЖЕНЕРНИХ АТАК

Легомінова С.В., д.е.н., проф., Стежко М.В.
Державний університет телекомунікацій
м. Київ, Україна

Новітні технології та інновації глибоко змінюють процес організації виробництва, створюють підґрунтя для стійкого зростання бізнес-можливостей. Разом з тим сучасні смарт-технології, інтелектуальний аналіз, хмарні технології обробки та збереження великих даних породжують нові загрози. Захист інформації набуває першочергової важливості. Витонченість і складність атак у кіберпросторі постійно вдосконалюються.

Одним із найбільш уразливих моментів у розвитку сучасного бізнесу виступає соціальна інженерія.

Соціоінжиніринг займає одне з перших місць за кількістю атак та зламів інформаційних систем компаній. Ексклюзивні конкурентні переваги досягаються шляхом здійснення розвідки, виявлення слабких сторін та вразливих ділянок організації, переманювання та підкупу співробітників, дискримінації конкурента, розкрадання інтелектуальної власності, конфіскації банківських рахунків та втрати споживачів унаслідок бізнес-збоїв, розкриття конфіденційної інформації, продажу особистої інформації на чорному ринку, порушення основних даних, викрадання даних клієнтів та їх продажу. Тому підприємства потребують нових методів боротьби, які б давали змогу оперативно відслідковувати та виявляти ознаки соціальної інженерії, попереджати кіберзагрози та протидіяти соціальному хакерству [1, с. 183].

Соціоінженерні атаки можуть бути вадкою загрозою для інформаційної безпеки, тому що вони спрямовані на використання людських слабкостей та довіри.

Для захисту від соціоінженерних атак необхідно розробляти та реалізовувати стратегії та методики, які дають можливість попереджати та виявляти атаки.

Методи аналізу захищеності користувачів інформаційних систем від соціоінженерних атак можуть включати аудит безпеки, соціальну інженерію, тестування вразливостей та інші техніки.

Співпраця між різними департаментами, такими як IT та HR, може бути корисною для запобігання соціоінженерним атакам, оскільки забезпечує раннє виявлення потенційних загроз.

Забезпечення освіти користувачів щодо соціоінженерних атак та їх наслідків може бути ефективним способом зменшення ризиків.

Системи захисту від соціоінженерних атак повинні бути проєктовані з урахуванням людського фактору, зокрема з використанням механізмів виявлення незвичайних або підозрілих дій користувачів.

Розроблення та використання політик безпеки, які включають в себе заходи щодо соціоінженерних атак, можуть знизити ризик зламу інформаційних систем.

Отже, ступінь захищеності від атак соціоінженерії залежить від новітніх знань, впровадження інноваційних інформаційних технологій з метою зниження ризиків та їх нівелювання. Процес захисту має поширюватись на всі ієрархічні рівні компанії, контроль за виконанням перманентно має виконувати ІТ-відділ.

Література

1. Половенко, Л., Мерінова, С. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації*. 2019. №10, С. 183-187. https://doi.org/10.37320/2415-3583/10.28

2. Соколов В.Ю., Курбанмурадов Д.М. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка.* 2018. № 1(1). С. 6–16.

3. Яковенко В.С., Казеян Н.К. Соціальна інженерія в Інтернет-просторі. *Вісник Чернівецького торговельно-економічного інституту. Економічні науки.* 2016. Випуск III–IV (63–64). С. 119–126.

ПЕНТЕСТИ ЯК ЗАСОБИ ПЕРЕВІРКИ ТЕХНІЧНОЇ СКЛАДОВОЇ ПРОЦЕСУ ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

Безсмертний О.Д.
Державний університет телекомунікацій
м. Київ, Україна

Сучасний світ неможливо уявити без новітніх технологій, які спрощують та автоматизують більшість процесів у майже всіх галузях. Сучасне навчання, медицину, різні сфери комунікації, та інші сфери неможливо уявити без використання сучасних технології. Проте через неймовірне поширення інформаційних комп'ютерних технологій світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інформаційної сфери щодо стороннього кібернетичного впливу.

Щоденно, згідно даних порталу *Threatmap* відбувається понад 30 мільйонів кібератак, використовуючи фішинг, методу «бекдор», соціальної інженерії, рекламного програмного забезпечення, та інших. В Україні від початку війни лише за 3 квартал 2022 року, за даними Держпецзв'язку[1] за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій інформаційної безпеки (ІБ) та 115 кіберінцидентів. Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програм-знищувачів.

З огляду на зростаючу тенденцію до кібератак за останні кілька років, важливо, щоб компанії усвідомлювали цю загрозу та могли виявляти вразливі місця у своїх системах. Кіберзагрози стають не тільки більш частими, але й більш витонченими. Кібербезпека актуальна для всіх людей у сучасному світі, включаючи політику надійних паролів для захисту ваших електронних листів або для компаній та інших організацій, які потребують захисту як пристроїв, так і даних від пошкоджень. Найбільш економічно ефективним способом зниження ризику кібератак є тестування на проникнення.

Тестування на проникнення, пентест (від англ. Penetration test) – це процес тестування комп'ютерної системи, мережі або веб-додатку для виявлення вразливостей, якими може скористатися зловмисник. Суть тесту на проникнення полягає у виявленні потенційних вразливостей, якими може скористатися зловмисник. Ідея полягає в тому, щоб перевірити слабкі місця, якими може скористатися зловмисник, а не системний адміністратор.

Пентест – це етична спроба перевірити й проаналізувати засоби захисту для захисту цих активів і частин інформації. Тест на проникнення передбачає використання тих самих інструментів, технік і методологій, які використовував би хтось зі зловмисними намірами. Це авторизований аудит безпеки та захисту комп'ютерної системи, узгоджений власниками систем. Законність проникнення в цьому сенсі досить чітка, тобто все, що виходить за рамки цієї угоди, вважається несанкціонованим.

Перед початком тесту на проникнення відбувається офіційне обговорення між тестувальником на проникнення та власником системи. Узгодження різних інструментів, технік та систем, які необхідно перевірити. Це обговорення формує сферу дії угоди про тестування на проникнення та визначає курс тестування на проникнення.

Література

1. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Київ : Держспецзв'язку, 2022. 18 с. URL: https://scpc.gov.ua/article/163.

СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

ЗАКОНОДАВЧА СТРУКТУРА ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ТА ЇЇ ВИКОРИСТАННЯ

Осаулов А.Р.
Державний університет телекомунікацій
м.Київ, Україна

У сучасну цифрову епоху інтернет та взаємопов'язані комп'ютерні системи відіграють дедалі важливішу роль у функціонуванні суспільства - від економіки до військової справи, особистого спілкування та розваг (European Union Agency for Cybersecurity, 2020). З огляду на критичну важливість цих систем, кіберстійкість стала критично важливим питанням. Кіберстійкість відображає здатність системи протистояти і відновлюватися після зловмисних кіберактивностей, таких як кібератаки, витоки даних і збої в роботі мережі (National Institute of Standards and Technology, 2021). Для забезпечення кіберстійкості необхідна законодавча та нормативна база, яка б містила керівні принципи, стандарти та найкращі практики для організацій, приватних осіб та урядів.

Уряди різних країн світу прийняли закони та нормативні акти для вирішення питання кіберстійкості. У Сполучених Штатах, наприклад, Федеральний закон про модернізацію інформаційної безпеки (FISMA) забезпечує комплексну основу для захисту федеральних інформаційних систем і даних (National Institute of Standards and Technology, 2014). Закон вимагає від федеральних відомств розробляти і впроваджувати програми інформаційної безпеки, проводити регулярну оцінку ризиків і дотримуватися мінімальних стандартів безпеки, встановлених Національним інститутом стандартів і технологій (NIST).

У Європі Загальний регламент захисту даних (GDPR) забезпечує комплексний набір правил для захисту персональних даних і приватності, включаючи кіберстійкість (European Union Agency for Cybersecurity, 2020). GDPR вимагає від організацій впроваджувати відповідні технічні та організаційні заходи для захисту персональних даних, повідомляти про порушення даних у відповідні органи протягом 72 годин, а також надавати особам певні права щодо їхніх даних.

На додаток до законів та підзаконних актів, міжнародні організації також встановили норми та стандарти кіберстійкості. Наприклад, Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (IEC) розробили низку стандартів для систем управління інформаційною безпекою, зокрема ISO/IEC 27001, який забезпечує комплексну основу для управління інформаційною безпекою (International Organization for Standardization, 2013).

Нормативні основи кіберстійкості

На додаток до законів і нормативних актів, нормативна база містить набір керівних принципів, найкращих практик і стандартів, яких організації повинні дотримуватися для забезпечення кіберстійкості. Наприклад, Національний інститут стандартів і технологій США (National Institute of Standards and Technology, 2021) пропонує набір керівних принципів для федеральних агентств, яких вони повинні дотримуватися при розробці своїх програм інформаційної безпеки (National Institute of Standards and Technology, 2021). Ці керівні принципи включають NIST Cybersecurity Framework, який забезпечує підхід до управління ризиками кібербезпеки, заснований на оцінці ризиків, і NIST SP 800-53, який забезпечує контроль безпеки для інформаційних систем (National Institute of Standards and Technology, 2014).

Іншим прикладом нормативної бази для забезпечення кіберстійкості є "Критичні елементи управління безпекою" (Critical Security Controls, CSC) Центру інтернет-безпеки (CIS), який надає пріоритетний набір дій для покращення загальної системи безпеки організації (Center for Internet Security, 2020). CSC надає стислий і практичний набір рекомендацій для організацій, яких вони повинні дотримуватися, включаючи рекомендації щодо управління активами, управління загрозами та вразливостями, контролю доступу та реагування на інциденти.

Підсумовуючи, можна сказати, що законодавчі та нормативні засади кіберстійкості створюють комплексну основу для забезпечення безпеки та стійкості комп'ютерних систем і мереж (European Union Agency for Cybersecurity, 2020). Ці основи містять набір правил, керівних принципів та найкращих практик, яких мають дотримуватися організації, окремі особи та уряди, та є важливими для забезпечення захисту критично важливої інфраструктури та даних суспільства від зловмисних кібератак (National Institute of Standards and Technology, 2021). Дотримуючись цих принципів, організації можуть вжити заходів для зменшення своїх ризиків.

Література

1. Center for Internet Security. (2020). CIS Controls. URL: https://www.cisecurity.org/controls/
2. European Union Agency for Cybersecurity. (2020). Cybersecurity in the European Union. URL: https://www.enisa.europa.eu/topics/cybersecurity-in-the-eu
3. International Organization for Standardization. (2013). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. Geneva, Switzerland: Author.
4. National Institute of Standards and Technology. (2014). Federal Information Security Modernization Act (FISMA). URL: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma
5. National Institute of Standards and Technology. (2021). Cybersecurity Framework. URL: https://www.nist.gov/cyberframework

6. National Institute of Standards and Technology. (2021). NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ЗАСТОСУВАННЯ ЕТИЧНИХ НОРМ СВІТОВИХ СТАНДАРТІВ В КОРПОРАТИВНОМУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Шуліпа Н.С., Порохницький О.А.
Державний університет телекомунікацій
м. Київ, Україна

Євроінтеграційні процеси в Україні, необхідність виходу вітчизняних підприємств з кризового стану потребують розробки механізму формування корпоративної інформаційної безпеки. Теоретичною основою є праці вітчизняних та закордонних вчених з питань управління інформаційною безпекою. Проблемними питаннями займались відомі дослідники Ж. Козінський, Т. Кобєлєва, М. Верес, С. Нагі, М. Сікорська, М. Мельник О. Панаско, О. Пригодюк. Їх дослідження сприяють підвищенню ефективності управління інформаційною безпекою [1].

Разом з тим, сьогодні бракує досліджень застосування в управлінні етичної складової за прикладом світових стандартів управління інформаційною та кібербезпекою.

Одним із організаційно-правових методів є комплаєнс – відносно нове поняття в діловому середовищі України. Комплаєнс (англ. compliance) – відповідність будь-яким внутрішнім або зовнішнім вимогам або нормам, в тому числі етичним. Відповідність законам, моральним правилам і стандартам у сфері комплаєнса зазвичай стосується таких питань, як дотримання належних стандартів поведінки на ринку, управління конфліктами інтересів, справедливе ставлення до клієнтів і забезпечення сумлінного підходу при консультуванні клієнтів. До сфери комплаєнса відносяться також специфічні області у сфері кібербезпеки, такі як: протидія легалізації доходів, отриманих злочинним шляхом, і фінансуванню тероризму; розробка документів і процедур, що забезпечують відповідність діяльності компанії з чинним законодавством; захист інформаційних потоків, протидія шахрайству і корупції, встановлення етичних норм поведінки співробітників і т. д. Запровадження комплаєнсу є ініціативою підприємства. Його наявність завжди засвідчує високу корпоративну культуру, прозорість та інноваційність в системі запровадження інструментів та технологій управління. Для підтримання стану захисту інформаційної безпеки в актуальному стані необхідно розвивати його далі – за допомогою сучасного, широкого та гнучкого каталогу сучасних заходів інформаційної безпеки [2-3].

Аналізуючи світові стандарти корпоративного управління інформаційної безпеки, необхідно зробити висновок про збільшення моральної складової в управлінні. Етичні норми – цінності та правила етики в управлінні

відображаються у корпоративних етичних кодексах, де закріплюються обов’язкові для усіх моральні принципи управління з урахуванням специфіки діяльності і яких повинні дотримуватися працівники організації в своїй діяльності.

Організаційна складова інформаційної політики, відображена в етичних кодексах допомагає гарантувати організації те, що кожен, хто пов'язаний із організацією, буде виконувати етичні корпоративні вимоги щодо забезпечення безпеки інформації. Фахівці з кібербезпеки, маючи доступ згідно своїх обов’язків до конфіденційної інформації, яка часто включає особисті персональні дані (наприклад, у сфері охорони здоров’я), цінної корпоративної інформації організації (банківська таємниця, …), повинні поводити себе етично і доводити своїм керівникам своїми діями, що вони гідні нагляду за цінною інформацією.

Світова практика застосування етичних стандартів у корпоративному управлінні почала застосовуватись ще з минулого століття [4]. Майже всі корпорації світу розробили великі корпоративні кодекси етики в галузі використання інформаційних технологій.

У США було проведено кілька обговорень, пов'язаних зі створенням і використанням на практиці загального кодексу етики, що зачіпає такі області. Близько 40% фірм, що входять до списку American Fortune 500, мають такі кодекси. У них закріплені інформаційні права і обов'язки стосуються питань використання e-mail в приватних цілях, моніторинг робочих місць, ставлення до корпоративної інформації і політики інформації про споживачів. У цих кодексах права власності та зобов'язання пов'язані з ліцензуванням програмного забезпечення, з власністю на інформацію, на програмне забезпечення, створене службовцями тієї чи іншої компанії, і з копіюванням програмного забезпечення. Закріплена також етика підзвітності і контролю, визначена індивідуальна відповідальність за якість інформаційних систем і якість діяльності – проектування робочих місць, ергономіка, задоволення потреб службовців. В кодексах закріплена мета – підвищити якість діяльності корпорації, поліпшення обслуговування споживачів і задоволеності службовців своїми робочими місцями.

Таким чином, сьогодні для інформаційної сфери в України існує нагальна потреба в розробленні етичних корпоративних кодексів, які на основі досвіду світових стандартів будуть забезпечувати підвищення ефективності управлінської діяльності забезпечення інформаційної безпеки організацій, підприємств та держави в цілому.

Література

1. Чубаєвський, В. Методи управління корпоративною інформаційною безпекою.. *Економіка та суспільство*, № 43 (2022). URL: https://doi.org/10.32782/2524-0072/2022-43-49

2. Kocziszky, György Compliance risk in the enterprise / G.Kocziszky, M.Veres Somosi, T.O.Kobielieva. Стратегії інноваційного розвитку економіки України: проблеми, перспективи, ефективність "Форвард–2017" : матерыали 8-ї Міжнар, наук.-практ. Internet-конф. студ. та молодих вчених, 27 грудня 2017 р. Харків : НТУ ХПІ, 2017. С. 54–57
3. Кобєлєва Т. О. Сутність та визначення комплаєнс-ризику. *Вісник Національного технічного університету ХПІ. Економічні науки.* 2020. № 1 (3). С. 116–121.
4. Martin Buss, «Penny-Wise Approach to Data Processing», *Harvard Business Review*, July - August 1981. Pp. 111-135

ЗАГАЛЬНІ ПРИНЦИПИ УПРАВЛІННЯ ПЕРСОНАЛОМ У СФЕРІ КІБЕРБЕЗПЕКИ

Бойко О.О.
Державний університет телекомунікацій,
Київ, Україна

Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Разом з тим, як свідчить аналіз [1], відсутність у значної частини відповідних структурних підрозділів навиків управління, необхідного кадрового забезпечення та належного контролю за кіберзахистом не дозволяє в сучасних умовах забезпечити роботу з організації надійного кіберзахисту держави.

Швидкий характер розвитку і взаємопов'язаність процесів в системі кібербезпеки потребує забезпечення оптимізованого підходу до розвитку працівників, що відповідають за управління ризиками у сфері кібербезпеки. Однак оскільки інформація і технології, включаючи багато новітніх типів операційної технології, стають дедалі складнішими та взаємопов'язаними між собою, може бути складно чітко описати роботу, яка виконується або яку ми бажаємо виконати, особливо у цих сферах.

У такій ситуації актуальним є необхідність чіткого визначення ролей та механізмів управління і взаємодії під час розв'язання завдань кібербезпеки. Одним із варіантів є напрацьовані фахівцями пропозиції загальних принципів управління персоналом у сфері кібербезпеки, відображені у Національній освітній ініціативі у сфері кібербезпеки (NICE) [2].

Загальні принципи NICE допомагають організаціям подолати проблему з описом своїх працівників для багатьох зацікавлених сторін шляхом використання підходу на основі стандартних блоків.

Управління персоналом у сфері кібербезпеки охоплює багато різних типів посад і різних типів організацій. До них належать органи державного сектору, приватні та некомерційні організації й організації, що надають послуги з освіти та тренінгів, розробники навчальних програм, постачальники сертифікатів, фахівці у сфері управління персоналом, менеджери з найму працівників, керівники окремих напрямів діяльності у кібербезпеці.

Загальні принципи управління персоналом у сфері кібербезпеки, що побудовані на основі набору окремих стандартних блоків, сформовані у вигляді Завдань, необхідних Знань та Навичок. Завдання описують роботу, яку потрібно виконати. Завдання визначають як діяльність, спрямовану на досягнення цілей організації, включаючи бізнес-цілі, технологічні цілі або цілі місії. Формулювання Завдань мають бути простими. Незважаючи на те, що робота, яка описана в Завданні, може складатися з багатьох етапів, як це показано на прикладі нижче, саме формулювання повинно легко читатися та розумітися.

Формулювання Знань пов'язані з формулюваннями Завдань тим, що тільки завдяки розумінню, наданому у формулюванні Знання, працівник буде здатним виконати Завдання. Знання визначаються, як набір понять в пам'яті, які можна відновити. Формулювання Знань можуть описувати базові або спеціальні поняття. Для виконання конкретного Завдання можуть знадобитися декілька формулювань Знань. Так само одне формулювання Знань може бути використане для виконання багатьох різних Завдань.

Формулювання Навичок пов'язані з формулюваннями Завдань тим, що працівник під час виконання завдань повинен продемонструвати певні навички. Хто не може продемонструвати описану навичку - не зможе виконати Завдання, яке потребує цю навичку. Навичка визначається як здатність виконувати спостережувану діяльність. Формулювання Навичок можуть описувати прості або складні навички. Декілька формулювань Навичок можуть знадобитися для виконання конкретного Завдання. Так само виконання Навички може застосовуватися для виконання більш ніж одного Завдання.

Важливим є також визначення у NICE застосування компетенцій. Компетенції надають організаціям механізм оцінювання учнів. Компетенції визначаються з використанням підходу на основі інтересів роботодавця, що забезпечує врахування унікального контексту організації. Крім того, компетенції допомагають організаціям, що надають послуги з освіти та підготовки фахівців кібербезпеки, реагувати на потреби роботодавця або галузі шляхом розроблення навчальних програм, які допомагають працівникам розвивати і демонструвати компетенції. Компетенції складаються з назви, опису компетенції, методу оцінювання, а також із групи пов'язаних формулювань знань, навичок та здібностей.

Багато організацій використовують команди для колективного вирішення складних проблем, об'єднуючи людей із доповнюючими навичками та досвідом.

Використовуючи різні ресурси і погляди, створені команди допомагають організаціям комплексно управляти ризиками. Команди використовують переваги спеціалізації знань та процесів кожного члена команди для ефективного розподілу роботи. Команди можуть бути визначені на основі робочих ролей або компетенцій.

Таким чином, використання загальних принципів NICE покращить комунікації стосовно того, як управляти персоналом, та, крім того, виявляти, набирати, розвивати та зберігати таланти у сфері кібербезпеки.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021.
URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 13.02.2023).
2. Petersen R. Workforce framework for cybersecurity (NICE framework) (ukrainian translation). National Institute of Standards and Technology, 2022.
URL: https://doi.org/10.6028/nist.sp.800-181r1.ukr (date of access: 13.02.2023).

ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Пальчинська В.Б., Щавінський Ю.В., к.т.н.
Державний університет телекомунікацій,
Київ, Україна

Завдяки глобальному сплеску інформаційних технологій у всіх сферах діяльності людини, суспільства і держави інформація стала вирішальним чинником, а в умовах сучасних глобальних та регіональних інформаційних протистоянь – знаряддям деструктивних комунікативних впливів, інформаційної експансії та агресії.

В умовах гібридної війни держава, що стала об’єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Інформаційна складова гібридної війни стає своєрідним фронтом ведення гібридних бойових дій. Внаслідок цього інформація в інформаційному середовищі піддається різноманітним загрозам, серед яких виділяють незаконний збір інформації, поширення дезінформації, засоби пропаганди, зміна інформаційної чистоти країною агресором та інформаційно-психологічний вплив як на власне населення так і на населення країни, що є суб’єктом агресії, а також на міжнародну спільноту [1].

В умовах знаходження України у стані гібридної війни домінуючою складовою є інформаційна війна, основним змістом якої є інформаційні

технології впливу на інформаційні системи з метою введення в оману масової чи індивідуальної свідомості, виведення з ладу критичної інформаційної інфраструктури, десинхронізацію процесів управління державою та її складовими. Тому сьогодні забезпечення інформаційної безпеки держави, як одної із складових національної безпеки, є актуальним завданням нарівні із веденням бойових дій на полі бою.

Забезпечення інформаційної безпеки, як одної із найважливіших функцій держави, закріплено у Конституції України [2]. Конституційні положення стали визначальними для розробки пакета нормативно-правових актів, необхідних для ефективного забезпечення інформаційної безпеки в Україні, в яких враховано основні положення міжнародних договорів та угод, ратифікованих Верховною Радою України. Нормативна база інформаційної безпеки спрямована на урегулювання відносин між суб'єктами інформаційної безпеки, закріплення їх правового статусу, порядку застосування сил та засобів забезпечення інформаційної безпеки тощо. Вона складається із Законів України, Постанов Верховної ради України і Кабінету Міністрів, указів Президента України стосовно інформаційної і кібербезпеки, нормативних документів у галузі технічного захисту інформації та державних стандартів України стосовно створення і функціонування комплексної системи захисту інформації.

Існуюча система нормативно-правових актів у сфері забезпечення інформаційної безпеки України спрямована на врегулювання, координації та взаємодії державних органів та інших суб'єктів забезпечення інформаційної безпеки України як на національному, так і на міжнародному рівнях. Інформаційна безпека у межах інформаційного законодавства розглядається з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам, механізмах усунення або запобігання таким загрозам правовими методами. У вітчизняному законодавстві, що регулює сферу інформаційної безпеки, відображені аспекти державної політики інформаційної безпеки, як механізм досягнення необхідних умов суспільного і державного життя в інформаційній сфері [4].

Разом з тим, аналізуючи специфіку правового забезпечення інформаційної безпеки держави, науковці відзначають деякі неузгодженості нормативно-правових актів як між собою, так і з чинною Конституцією. [3, с.133]. Потребують відображення у законодавчих актах питання посилення відповідальності за порушення інформаційної безпеки відповідно до викликів і загроз, пов'язаних з гібридною війною [5, 6].

Висока турбулентність, хаотизація, невизначеність безпекового середовища та неповнота знань є одними з головних рис гібридної сучасності та викликами для системи забезпечення інформаційної безпеки. Помилки та неповне охоплення всього діапазону інформаційних загроз може зумовити відсутність потрібних захисних спроможностей і неефективність всієї системи забезпечення національної безпеки [7].

Є об'єктивна потреба в опрацюванні базового закону – Інформаційного кодексу, який би включав окремий розділ про інформаційну безпеку чи

прийнятті спеціального Закону України «Про інформаційну безпеку України», який зможе регламентувати основні засади державної політики, спрямованої на захист інформаційної безпеки людини, суспільства та держави від зовнішніх та внутрішніх загроз.

Доцільно законодавчо визнати інформаційну безпеку України як комплекс системних превентивних заходів із надання гарантій захисту життєво важливих інтересів особистості суспільству і державі від негативних інформаційних впливів, пов'язаних з інформаційними війнами.

Таким чином, поряд із досягненнями в удосконаленні правових механізмів у сфері забезпечення інформаційної безпеки, сьогодні є ще багато проблем, які потребують оперативного регулювання у правовому полі з урахуванням сучасних викликів у зв'язку з гібридною війною проти України.

Література

1. Інформаційна безпека держави у контексті протидії інформаційним війнам : навч. посіб. / ред. В. Б. Толубко. Київ : НАОУ, 2004. 315 с.
2. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 13.02.2023).
3. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2012. № 3. С. 132–137.
4. Качковська Л., Малеончук Г., Зінюк Д. Інформаційний вплив в умовах гібридної війни. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022. № 3 (14). С. 87–102. URL: https://doi.org/10.29038/2524-2679-2022-03-87-102 (дата звернення: 30.03.2023).
5. Марущак А. І. European experience of offense prevention in the information sphere. *Ukrainian scientific journal of information security*. 2019. Т. 25, № 1. URL: https://doi.org/10.18372/2225-5036.25.13665 (дата звернення: 17.02.2023).
6. Fostering freedom online: the role of Internet intermediaries / R. MacKinnon et al. United States : UNESCO, 2014. 210 p.
7. Сунгуровський М. В. Чого бракує та що потрібно для побудови ефективної системи інформаційної безпеки. *Інформаційна безпека: сучасний стан, проблеми та перспективи* : матеріали Міжнар. Науково-практ. Конф., м. Київ, 20 берез. 2023 р. Київ, 2019. С. 12–14.

СУЧАСНИЙ ДИСКУРС ЩОДО РИЗИКІВ КІБЕРБЕЗПЕКИ

Гайдур Г.І., д.т.н., проф., Скибун О.Ж.
Державний університет телекомунікацій,
Київ, Україна

На сьогодні постійно зростає рівень цифровізації, комп'ютеризації та віртуалізації усіх сфер суспільства (економічної, політичної, соціальної та гуманітарної) та суспільних відносин. Подальший розвиток та широке використання цифрових, інформаційно-комунікаційних та інформаційних технологій разом із міжнародними електронними комунікаційними мережами і глобальною мережею передачі даних формують нову цифрову віртуальну реальність та кіберпростір, де інформація виступає товаром і стратегічним ресурсом, а робота з нею створює нові виробничі процеси та засоби виробництва. Вказане стає основним трендом останніх десятиліть, де все більша кількість суб'єктів працює із цифровою інформацією, базами даних, коли багато технологічних процесів, процесів управління на виробництві та процесів управління функціонування багатьох компаній будуються на базі цифрових віртуальних технологій із використанням корпоративних інформаційно-комунікаційних систем та мереж. На сьогодні у сферах надання послуг, торгівлі та логістики багатьох глобальних транснаціональних корпорацій використовуються нові технологічні рішення, побудовані на застосуванні можливостей Інтернету речей, штучного інтелекту, робототехніки тощо. Це створює передумови для збільшення рівня кіберінцидентів та активності кібершахраїв, а тому кіберскладова починає все більше впливати на рівень ризиків ведення бізнесу, адже «ризик представляє собою можливі втрати, поразку, небезпеку, несприятливі події або наслідки» [4]. При цьому нові кіберризики трансформуються у групи, а саме Так, вже у 2020 році кіберризики досягли відмітки у 78 відсотків на фоні усіх інших ризиків, що підтверджує тезу про те, що в рамках зростання темпів «цифровізації економічного та суспільно-політичного життя, ризики, пов'язані з кібербезпекою, стають ключовими бізнес-ризиками», а кібербезпека при цьому стає «важливою частиною інформаційної безпеки підприємства», а «джерелами ризиків в даному процесі виступають як хакерські атаки, дії кіберзлочинців, так і необережні чи навмисні дії самих працівників та внутрішніх користувачів інформаційних систем підприємства, які не дотримуються встановлених процедур, правил й спричиняють негативні наслідки» [4]. Ось чому «система захисту інформації і кібербезпеки (далі – СЗІКБ) – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки», а тому «оцінка ефективності може здійснюватися в процесі створення, приймання та експлуатації СЗІКБ» [5, с.125]. При цьому необхідно зважати, що «традиційні підходи до забезпечення виявлення та реагування на загрози не встигають за обсягом, різноманітністю та швидкістю сучасних загроз» [3], особливо, коли мова йде про кібезагрози та кіберизики. А тому для того «щоб зберегти цілісність даних та уникнути

серйозних збоїв, компаніям слід враховувати кібербезпеку та конфіденційність при розробці нових видів діяльності», що «включає в себе» перш за все «узгодження безпеки даних з бізнес-цілями, залучення необхідних спеціалістів і участь кіберкоманди у розробці нових проєктів» [3]. А тому можна говорити, що «діяльність СЗІКБ із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п'яти функцій кібербезпеки: ідентифікація ризиків, кіберзахист; виявлення кіберінцидентів; реагування; відновлення поточного стану кібербезпеки» [5, с.126]. При цьому необхідно враховувати, що кіберзазгрози та кіберінциденти не є статичною величиною, вони трансформуються та змінюються. Наприклад у 2021 році відбувалися «атаки на ланцюжки поставок і на третіх осіб (3rd parties); атаки на елементи «інтернету речей», системи захисту хмарних інфраструктур, безпеку персональних даних (в тому числі біометричних)», а для протидії «ransomware і кріптомайнерам» [1] та в інформаційній безпеці в цілому почав широкого використовуватися штучний інтелект. А вже «у 2022 році зросла загроза програм-вимагачів, хакери почали частіше користуватися вразливостями в програмному забезпеченні для захоплення комп'ютерних серверів, а також продовжувалися витоки даних, зокрема в таких компаніях, як Uber, Microsoft і LastPass. Згідно зі звітом Identity Theft Resource Center, за перші дев'ять місяців минулого року було зареєстровано 1291 випадків компрометації даних, що вплинуло на близько 166,8 мільйонів людей.» [3]. В свою чергу «аналітики Gartner виділяють сім основних тенденцій кібербезпеки, що були актуальними в 2022 році, проаналізувавши які, компанії зможуть краще протистояти новим ризикам у 2023-му», а саме «розширення поверхні атаки; захист систем ідентифікації; ризики при постачанні програмного забезпечення; консолідація постачальників; сітка служб кібербезпеки; розподілені рішення; людина, як і раніше, є «слабкою ланкою»» [3]. Так, О. Бакалінська відзначає, що «найбільше увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів» [2, с.87]. Так, С. Семенова вважає, що для «зменшення ризиків у кіберпросторі до прийнятного рівня» та/або «нейтралізації потрібна низка важливих і взаємопов'язаних дій», серед яких автор виділяє такі: «інвестиції в досконалі технічні засоби безпеки, їхнє належне обслуговування і оновлення; навчання кадрів, як користувачів інформаційних систем, проведення тренінгів, встановлення суворих регламентів і процедур поводження з інформацією та ІТ системами» тощо [4]. При цьому для «протидії підприємства найбільшим ризиками необхідно враховувати специфіку і сферу діяльності компанії, її розмір, середовище та взаємодію з внутрішніми і зовнішніми користувачами, регламент управління ризиками загалом та готовність до кожного» [4]. Крім того щоб «бути попереду» кібершахраїв необхідно застосовувати новітні розробки, наприклад «Новим глобальним фінтех-трендом, як вважають експерти, може стати Ransom-as-a-Service (RaaS). RaaS, завдяки використанню технологій Big

Data та Machine Learning, може надати критично важливі дані про операції з відмивання грошей відділу, що відповідає за комплаєнс у компанії. Крім того, RaaS може знизити адміністративні витрати, забезпечити фінансову стабільність та убезпечити клієнтів від порушення цілісності даних.» [3].

Отже можна відзначити, що разом із цивілізаційним прогресом зростає і рівень кіберзагроз для тих компаній, які використовують цифрові комп'ютерні віртуальні технології для ведення бізнесу, взаємодії із споживачами послуг та управління бізнес-процесами. Так, тренди кіберризиків формуються на базі появи та використання новітніх технологій, технологічного обладнання та появі нових програмних продуктів і послуг. А тому питання протидії кіберзагрозам для мінімізації кіберризиків починає домінувати. Для досягнення успіху необхідно підходити комплексено до питань кібербезпеки та кіберзахисту як на технологічному, технічному, так і людському рівнях.

Література

1. Актуальні тренди кібербезпеки в 2021 році. *Построение и настройка компьютерной корпоративной и домашней сети в Киеве*. URL: http://www.telesphera.net/blog/aktyalnie-trendy-kiberbezpeki-v-2021.html (дата звернення: 15.02.2023).
2. Бакалинська О. О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. Т. 9. С. 100–108. URL: https://doi.org/10.32849/2663-5313/2019.9.17. (дата звернення – 13.02.2023).
3. Кібербезпека як ключовий фінтех-тренд року: що варто знати про загрози та захист - Fintech Insider. *Fintech Insider - Дізнавайся першим*. URL: https://fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/ (дата звернення: 13.02.2023).
4. Семенова С. М. Ключові тенденції в управлінні ризиками провідних компаній єс за оцінками внутрішніх аудиторів. *Ефективна економіка*. 2020. Т. 9. https://doi.org/10.32702/2307-2105-2020.9.68 (дата звернення – 13.02.2023).
5. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури / Ю. І. Хлапонін та ін. *Кібербезпека: освіта, наука, техніка*. 2022. Т. 3, № 15. С. 124–134. URL: https://doi.org/10.28925/2663-4023.2022.15.1241341

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ КЕП, УЕП У БАНКІВСЬКИХ УСТАНОВАХ

Голобородько С.О., Харитончук М.
Державний університет телекомунікацій
м. Київ, Україна

Електронний підпис — це електронні дані, які забезпечують цілісність документів та ідентифікують особу. Електронний підпис може зберігатися у вигляді MobileID, підпису на ID-картці, підпису на "токені" чи захищеному носії інформації.

За допомогою електронного підпису можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо. Документи з цим підписом мають таку саму юридичну силу, як і документи, підписані власноруч.

У банківській системі України застосовуються кваліфікований ЕП, удосконалений ЕП, ЕП Національного банку, простий ЕП, кваліфікована електронна печатка, удосконалена електронна печатка.

Кваліфікований електронний підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. КЕП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Зберігається КЕП на спеціальних засобах КЕП.

Засіб КЕП – це спеціальна захищена флешка, на якій крім сертифікатів не може зберігатися нічого. Доступ до них закрит і можливий лише за допомогою спеціального програмного забезпечення та із занням пароля або резервного пароля для відновлення. В іншому випадку після введення декількох неправильних пін-кодів, носій блокується без можливості відновлення.

Засіб КЕП є засобом криптографічного захисту інформації та мусить мати експертний висновок за результатами державної експертизи у сфері захисту інформації. Перелік таких засобів наведено на порталі Держспецзв'язку. Акредитовані виробники токенів та смарткарт Токени "Автор", АТ “ІІТ”.

УЕП — це е-підпис, створений внаслідок криптографічного перетворення е-даних із використанням засобу УЕП, який дає змогу здійснити е-ідентифікацію підписувача та виявити порушення цілісності е-даних, з якими пов’язаний цей е-підпис.

Тому для підписання конфіденційної інформації краще використовувати КЕП оскільки носій є захищеним від копіювання, зміни, захищений паролем.

Література

1. Що таке електронний підпис? URL: https://diia.gov.ua/faq/2.
2. Використання кваліфікованих та удосконалених е-підписів URL: https://czo.gov.ua/edp-legislation-clarification?id=2.
3. Про затвердження Положення про застосування електронного підпису в банківській системі України URL:https://zakon.rada.gov.ua/laws/show/v0078500-17#Text.

ШТУЧНИЙ ІНТЕЛЕКТ В УПРАВЛІННІ РИЗИКАМИ КІБЕРБЕЗПЕКИ

Сокуренко Д.О
Державний університет телекомунікацій
м. Київ, Україна

Розвиток штучного інтелекту (ШІ) кардинально змінив підхід організацій до кібербезпеки. Рішення з кібербезпеки на основі штучного інтелекту можуть виявляти загрози та реагувати на них швидше й точніше, ніж будь-коли раніше. Однак із збільшенням повноважень зростає відповідальність. Організації повинні переконатися, що їхні рішення з кібербезпеки на основі штучного інтелекту належним чином керуються та керуються для забезпечення безпеки їхніх систем і даних.

Завдання управління кібербезпекою на основі штучного інтелекту є подвійним. По-перше, організації повинні переконатися, що їхні рішення на основі ШІ належним чином налаштовані та керовані ними. Це включає в себе переконання, що алгоритми штучного інтелекту належним чином навчені та оновлені, а дані, які використовуються для навчання алгоритмів, є точними та актуальними. Крім того, організації повинні переконатися, що їхні рішення на основі ШІ належним чином контролюються та перевіряються, щоб переконатися, що вони працюють належним чином.

Друга проблема управління кібербезпекою на основі штучного інтелекту полягає в тому, щоб рішення відповідали чинним законам і нормам. Оскільки рішення на основі штучного інтелекту стають потужнішими, вони також повинні дотримуватися дедалі суворіших правил конфіденційності та безпеки даних. Організації повинні переконатися, що їхні рішення на основі штучного інтелекту відповідають чинним законам і нормам, а також що вони належним чином перевіряються та контролюються для забезпечення відповідності.

Організації також повинні переконатися, що їхні рішення на основі ШІ захищені від зловмисників. Рішення на основі ШІ особливо вразливі до зловмисних атак, оскільки зловмисники можуть використовувати алгоритми ШІ, щоб отримати доступ до конфіденційних даних або маніпулювати алгоритмами у власних цілях. Організації повинні переконатися, що їхні рішення на основі штучного інтелекту належним чином захищені та контролюються для виявлення зловмисної діяльності та реагування на неї.

Нарешті, організації повинні переконатися, що їхні рішення на основі ШІ є етичними та відповідальними. Рішення на основі штучного інтелекту можуть мати глибокий вплив на суспільство, і організації повинні переконатися, що їхні рішення розробляються та використовуються відповідально. Це включає забезпечення належного навчання та перевірки алгоритмів, щоб уникнути небажаних наслідків, а також те, що дані, які використовуються для навчання алгоритмів, є точними й актуальними.

Проблеми управління кібербезпекою на основі штучного інтелекту є значними, але вони не є непереборними. Завдяки правильній політиці та процедурам організації можуть забезпечити належне керування, моніторинг і

захист їхніх рішень на основі ШІ. Вживаючи необхідних заходів для забезпечення безпеки та відповідності своїх рішень на основі штучного інтелекту, організації можуть гарантувати, що їхні системи та дані залишатимуться безпечними та захищеними.

Оскільки використання штучного інтелекту (ШІ) в управлінні кібербезпекою продовжує зростати, також зростають нормативні наслідки цієї технології. Системи управління кібербезпекою на основі штучного інтелекту все частіше використовуються для виявлення кіберзагроз і реагування на них, і хоча ця технологія має потенціал для значного підвищення безпеки, вона також викликає питання щодо конфіденційності, захисту даних і відповідності.

Щоб переконатися, що системи управління кібербезпекою на основі штучного інтелекту відповідають існуючим нормам, уряди та організації повинні застосовувати проактивний підхід до розуміння наслідків цієї технології. Це включає розуміння можливостей використання систем на основі штучного інтелекту для зловмисних цілей, а також можливості використання систем на основі штучного інтелекту для моніторингу та контролю за діяльністю користувачів.

Крім того, організації повинні враховувати наслідки систем управління кібербезпекою на основі ШІ для конфіденційності та захисту даних. Системи на основі штучного інтелекту здатні збирати й аналізувати великі обсяги даних, і ці дані потрібно обробляти відповідно до існуючих правил. Організації також повинні гарантувати, що системи на основі ШІ не використовуються для дискримінації певних користувачів або груп.

Нарешті, організації повинні розглянути наслідки систем управління кібербезпекою на основі ШІ для відповідності. Системи на основі штучного інтелекту здатні приймати рішення та виконувати дії, які можуть мати значні наслідки для дотримання існуючих правил. Організації повинні переконатися, що системи на основі штучного інтелекту належним чином налаштовані та контролюються для забезпечення відповідності існуючим нормам.

Оскільки системи управління кібербезпекою на основі штучного інтелекту стають все більш поширеними, важливо, щоб організації та уряди використовували проактивний підхід до розуміння наслідків цієї технології. Розуміючи потенційні наслідки систем на основі штучного інтелекту, організації можуть переконатися, що вони відповідають існуючим нормам і захищають дані своїх користувачів.

Оскільки організації все більше покладаються на цифрові технології, потреба в надійному управлінні кібербезпекою стає більш важливою, ніж будь-коли. Штучний інтелект (ШІ) відіграє все більш важливу роль у допомозі організаціям посилити управління кібербезпекою та захистити свої цифрові активи.

ШІ можна використовувати для автоматизації процесу виявлення та реагування на кіберзагрози. Використовуючи аналітику на основі ШІ, організації можуть швидко виявляти підозрілу активність і реагувати на неї в режимі реального часу. AI також можна використовувати для виявлення шкідливого

програмного забезпечення та зловмисників, допомагаючи організаціям захистити свої мережі від зловмисних атак.

ШІ також можна використовувати для підвищення точності політик і процедур безпеки. Використовуючи аналітику на основі штучного інтелекту, організації можуть краще зрозуміти загрози, з якими вони стикаються, і розробити ефективніші політики та процедури безпеки. ШІ також можна використовувати для автоматизації процесу забезпечення виконання політик і процедур безпеки, допомагаючи організаціям переконатися, що їх політики безпеки дотримуються.

Нарешті, ШІ можна використовувати для підвищення ефективності аудитів безпеки. Використовуючи аналітику на основі штучного інтелекту, організації можуть краще розуміти стан безпеки своїх мереж і визначати області, де їм потрібно покращити. ШІ також можна використовувати для автоматизації процесу проведення перевірок безпеки, допомагаючи організаціям швидко виявляти та усувати будь-які вразливості безпеки.

Загалом штучний інтелект відіграє все більш важливу роль у допомозі організаціям посилити управління кібербезпекою та захистити свої цифрові активи. Використовуючи аналітику на основі штучного інтелекту, організації можуть швидко виявляти підозрілу активність, запроваджувати політики та процедури безпеки та підвищувати ефективність перевірок безпеки. Штучний інтелект допомагає організаціям захистити свої мережі від зловмисних атак і переконатися, що їх політики безпеки дотримуються.

Розвиток штучного інтелекту (ШІ) кардинально змінив правила багатьох галузей, і кібербезпека не стала винятком. Штучний інтелект має потенціал кардинально змінити спосіб управління ризиками кібербезпеки організацій, спрощуючи виявлення загроз і реагування на них у реальному часі.

Рішення на основі ШІ вже використовуються для автоматизації багатьох виснажливих і трудомістких завдань, пов’язаних з управлінням ризиками кібербезпеки. Використовуючи автоматизацію на основі штучного інтелекту, організації можуть швидко виявляти потенційні загрози та реагувати на них, що дозволяє їм бути на випередженні та зменшувати ризики.

ШІ також можна використовувати для аналізу великих обсягів даних, щоб виявити шаблони та аномалії, які можуть свідчити про потенційне порушення безпеки. Це дозволяє організаціям раніше виявляти загрози та швидше реагувати, зменшуючи кількість завданої шкоди.

Рішення на основі штучного інтелекту також можна використовувати для виявлення та визначення пріоритетів уразливостей, дозволяючи організаціям зосередити свої ресурси на найактуальніших загрозах. Це може допомогти організаціям зменшити загальний ризик і забезпечити актуальність заходів безпеки.

Загалом штучний інтелект має потенціал кардинально змінити спосіб управління ризиками кібербезпеки організацій. Використовуючи автоматизацію на основі штучного інтелекту, організації можуть швидко виявляти потенційні загрози та реагувати на них, виявляти закономірності та аномалії та визначати

пріоритети вразливостей. Це може допомогти організаціям зменшити ризики та забезпечити актуальність заходів безпеки.

Література

1. Штучний інтелект у телекомунікаційних компаніях URL:https://www.cfo.com/issledovaniya/index.php?arti cle=39568/(дата звертання 26.05.2020);
2. Навчальний посібник «Методи та системи штучного інтелекту» Лубко Д.В. Шаров С.В.//Напрямки використання штучного інтелекту//2019 -ст. 16-25;
3. Глибовець М.М., Олецький О.В. Системи штучного інтелекту.- Київ: Видво«КМ Академія», 2002. 366 с;

ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Мартинова Ю. В.
Державний університет телекомунікацій
м. Київ, Україна

В умовах постійного розвитку інформаційних технологій та зростання загроз кібербезпеки питання ефективного управління подіями в сфері інформаційної безпеки набуває особливої актуальності для підприємств. Цей аспект вимагає детального аналізу сучасних методів управління подіями та їхнього застосування на практиці. У даному дослідженні розглядається роль та значення таких методів у контексті забезпечення інформаційної безпеки на підприємствах.

Сучасні методи управління подіями в інформаційній безпеці охоплюють широкий спектр інструментів та технологій. Серед них варто відзначити системи моніторингу, аналізу логів, виявлення вторгнень, та інші інструменти, які допомагають вчасно реагувати на потенційні загрози. Важливо також враховувати аспекти автоматизації та інтеграції цих методів для оптимізації роботи з інформаційною безпекою

Проведений аналіз використання сучасних методів управління подіями на підприємствах показує, що багато компаній вже впроваджують подібні системи. Однак, існують виклики, такі як нестача кваліфікованих кадрів, неоптимальна конфігурація інструментів, а також несистемний підхід до розгляду інформаційної безпеки на рівні підприємства.

З урахуванням виявлених проблем та недоліків пропонуються конкретні рекомендації щодо вдосконалення систем управління подіями на підприємстві. Це може включати в себе підвищення кваліфікації персоналу, оптимізацію конфігурації інструментів, а також впровадження інтегрованих підходів до управління інформаційною безпекою.

Дослідження сучасних методів управління подіями в інформаційній

безпеці на підприємстві дозволило зрозуміти важливість цього аспекту для забезпечення надійності та стійкості інформаційних систем. Реалізація ефективного управління подіями вимагає комплексного підходу, системної роботи та постійного вдосконалення. Підводячи підсумок, можна визначити, що правильно налаштована система управління подіями є ключовим елементом сучасної інформаційної безпеки підприємства.

Література

1. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Вісник Хмельницького національного університету. URL: https://forinsurer.com/news/18/01/26/35755?hl=%C1%E0%F0%EE%EC%E5%F2%F0
2. ЗУ «Про інформацію» від 02.10.1992 (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650) URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/3980
3. Four Key Components of a Strong Insider Threat Management Strategy - Exabeam URL: https://www.exabeam.com/information-security/four-key-components-of-a-strong-insider-threat-management-strategy/

ОСОБЛИВОСТІ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Городничий В.В.
Державний університет телекомунікацій
м. Київ, Україна

Інформаційні технології стали невід'ємною частиною сучасного бізнесу, відкриваючи нові можливості, але й насамперед ставлячи перед підприємствами серйозні виклики. Одним із найбільших викликів є збільшення ризиків інформаційної безпеки, пов'язаних з недостатньою захищеністю конфіденційної інформації. Управління ризиками інформаційної безпеки стає стратегічною необхідністю для забезпечення стійкості організації в умовах сучасного інформаційного середовища.

Однією з основних особливостей управління ризиками інформаційної безпеки є постійна зміна загроз і технологічного оточення. Кіберзлочинці постійно удосконалюють свої методи атак, тому стратегії управління ризиками повинні бути гнучкими і постійно адаптуватися до нових викликів. Перехід до облачних технологій, використання Інтернету речей та інших інноваційних рішень робить управління ризиками більш складним і вимагає постійного моніторингу. [1]

Ще однією важливою особливістю є необхідність узгодженого підходу до управління ризиками на всіх рівнях організації. Інформаційна безпека не може бути відокремленою функцією від інших бізнес-процесів. Застосування інтегрованого підходу вимагає співпраці між відділами, включаючи високе керівництво, власників бізнес-процесів і фахівців із інформаційної безпеки.

Управління ризиками інформаційної безпеки передбачає не лише захист від потенційних загроз, але й ефективне використання можливостей. Забезпечення балансу між безпекою та доступністю є ключовим аспектом управління ризиками. Важливо враховувати, що деякі ризики можуть бути прийняті для забезпечення більшої ефективності та інноваційності. [2]

Особливості регулювання інформаційної безпеки, зокрема відповідність стандартам та законодавству, також визначають особливості процесів управління ризиками. Компанії повинні бути готові до виконання вимог регуляторів і впровадження стандартів, що регулюють зберігання і обробку конфіденційної інформації. [3]

Управління ризиками інформаційної безпеки – це складний і постійно змінюючийся процес, який вимагає не лише технічної експертизи, але й стратегічного бачення та спроможності адаптуватися до нових реалій. Лише інтегрований та узгоджений підхід може забезпечити ефективний захист від загроз інформаційної безпеки, забезпечуючи сталість та розвиток організації в цифровому світі.

Література

1. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою. Дніпро: 2020. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf

2. Залога В. О. Стандарти в галузі управління ризиками інформаційної безпеки. Суми: 2014. URL: http://essuir.sumdu.edu.ua/handle/123456789/40088

3. Гуменюк В. В. Методи підвищення ефективності управління ризиками інформаційної безпеки підприємства. Тернопіль: 2019. URL: http://elartu.tntu.edu.ua/handle/lib/30728

СПОСОБИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННІ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Ухань Я.В., Сокуренко Д.О.
Державний університет телекомунікацій
м. Київ, Україна

В сучасному цифровому світі зростаючий вплив штучного інтелекту супроводжується постійним удосконаленням кібератак та інших форм кіберзлочинності. Разом з тим, штучний інтелект стає важливим інструментом

у боротьбі з кіберзагрозами та способом вдосконалення систем управління кібернетичною безпекою організацій.

Використання алгоритмів машинного навчання, глибокого навчання та аналізу великих обсягів даних дозволяє ефективно виявляти, прогнозувати та запобігати кібератакам. Застосування ШІ також дозволяє підвищити швидкість реакції на інциденти та створювати адаптивні системи, які самостійно коригуються відповідно до характеру кіберзагроз, що постійно змінюються.

Особливу загрозу сьогодні хакерські атаки складають для на Інтернету речей (IoT) та транспортних засобів. IoT – це не тільки розумний дім, це поняття включає і віддалений контроль за допомогою сенсорів за технологічними процесами виробництва з передачею даних мережевою інфраструктурою [1].

За останні кілька років рішення штучного інтелекту швидко розвинулися до такої міри, що вони можуть принести значну користь операціям кіберзахисту в широкому спектрі організацій і місій. Автоматизуючи ключові елементи основних функцій, що вимагають великої кількості праці, штучний інтелект може перетворити робочі кіберпроцеси на оптимізовані, автономні, безперервні процеси, які прискорюють виправлення та максимізують захист.

Штучний інтелект (англ. Atificial Intelligence, AI) та машинне навчання (англ. Machine learning, ML) все частіше використовуються в кібербезпеці для виявлення загроз, реагування та автоматизації завдань безпеки. Науковці одноголосно стверджують, що такі проблеми, як змагальне машинне навчання, упередження в алгоритмах штучного інтелекту та потенціал атак, керованих штучним інтелектом, повинні бути ретельно розглянуті та пом'якшені [2-3]. Штучний інтелект може підвищити швидкість виявлення, відстежуючи внутрішні та зовнішні джерела інформації та швидко співвідносячи цю інформацію для виявлення незвичайних дій, щоб мінімізувати наслідки. Штучний інтелект може покращити автентифікацію користувачів за допомогою фізичної біометрії, поведінкової біометрії або багатофакторної автентифікації захищаючи імена користувачів, паролі і навіть одноразові текстові токени.

Одним із відомих інструментів, які використовують організації для виявлення кіберзагроз є системи UEBA - Аналітика поведінки користувачів і сутностей, які зосереджені на моніторингу та аналізі поведінки користувачів в організації з метою виявлення зловмисної або несанкціонованої активності. Використовуючи ШІ UEBA можна застосувати для доповнення або заміни традиційних методів безпеки, таких як системи виявлення вторгнень (IDS), надаючи більш повне уявлення про діяльність в організації швидкість реакції. Разом з тим, науковці відзначають, що розроблені на основі ШІ моделі безпеки сторонніми організаціями необхідно постійно удосконалювати та пристосовувати як до потреб організації так і до постійно мінливих кіберзагроз, що потребує особливих знань в області кібербезпеки та програмування. Одним із варіантів вирішення цієї проблеми є розроблення власних моделей на основі ШІ для конкретної організації з її завданнями.

В середовищі програмування мови PYTHON є велика кількість стандартних бібліотек з готовими блоками коду, які можна використовувати для створення систем управління кібернетичною безпекою:

- бібліотеки для роботи з мережевим трафіком *Scapy* для захоплення та аналізу мережевого трафіку;
- бібліотеки для роботи з журналами подій (Event Logs) - *win32evtlog* в операційних системах Windows або *syslog* для операційних систем на базі UNIX;
- бібліотеки для збору даних з веб-сайтів *requests, BeautifulSoup* або Scrapy (це може бути корисно для виявлення загроз, які можуть бути пов'язані з онлайн-активністю);
- бібліотеки *pandas ma scikit-learn* для обробки та очищення даних, видалення аномалій і кодування категоріальних змінних;
- бібліотеки TensorFlow та Keras для створення Глибокої Нейронної Мережі (ГНМ) для виявлення кіберзагроз;

При цьому необхідно пам’ятати, що застосування машинного навчання для виявлення кібератак – це динамічний процес, і важливо постійно вдосконалювати моделі та методи для ефективного протистояння зростаючим кількісно та якісно кіберзагрозам.

Таким чином, застосування штучного інтелекту в кібербезпеці може значно підвищити ефективність автоматизованого управління системами кібербезпеки організацій і потребує подальших наукових досліджень.

Література

1. Kimani K., Oduol V., Langat K.. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.,* 25 2019, pp. 36-49, URL: https://doi.org/10.1016/j.ijcip.2019.01.001
2. Cheng Y.-L., Lee C.-Y., Huang Y.-L., Buckner C.A. Smart health and cybersecurity in the era of artificial intelligence. *Intech,* 11 (2016), p. 13. URL: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics (дата звернення 24.11.2023 р.)
3. Yazdinejad A., Kazemi M., Parizi R.M., Dehghantanha A., Karimipour H.. An ensemble deep learning model for cyber threat hunting in industrial internet of things. *Digit. Commun. Netw.,* 9(1), 2022. pp. 101-110. URL: https://doi.org/10.1016/j.dcan.2022.09.008

КІБЕРБЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ БІЗНЕСУ: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПІДХОДІВ ТА МЕТОДІВ

Гундер А.М.
Державний університет телекомунікацій
м. Київ, Україна

Кібербезпека та кіберстійкість є ключовими компонентами для забезпечення безпеки бізнесу. Вони допомагають захистити дані, системи та мережі від кібератак, а також забезпечити відновлення після кібератак.

Кібербезпека - це практична діяльність, спрямована на захист комп'ютерних систем і мереж від кібератак. Вона включає в себе весь комплекс заходів - від керування паролями до інструментів комп'ютерної безпеки на основі технологій машинного навчання [1].

Кібербезпека насамперед зосереджена на запобіганні й захисті комп’ютерних систем, мереж і даних від цифрових атак, несанкціонованого доступу й інших загроз. Охоплює широкий спектр методів, технологій і процесів, призначених для захисту цілісності, конфіденційності та доступності даних.

Заходи кібербезпеки спрямовані на запобігання загрозам шляхом захисту систем від несанкціонованого доступу або атак включають розгортання брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS).

Значною частиною кібербезпеки є виявлення потенційних ризиків, оцінка їхньої ймовірності та впливу, а також вжиття заходів для їх пом’якшення. Оцінка ризиків і сканування вразливостей є звичайними методами кібербезпеки.

Кібербезпека передбачає дотримання політик, стандартів і правових вимог. Щоб захистити конфіденційну інформацію, організаціям часто потрібно дотримуватися таких нормативних актів, як GDPR, HIPAA або PCI-DSS.

Підходи до забезпечення кібербезпеки бізнесу значною мірою залежать від технологічних рішень. Вони зосереджені на впровадженні апаратних і програмних продуктів, які захищають від відомих вразливостей і загроз.

Хоча технології відіграють вирішальну роль, навчання користувачів і персоналу компанії безпечній поведінці в Інтернеті та “кібергігієні” також є фундаментальною частиною стратегії кібербезпеки.

Кібербезпека включає розробку плану реагування на інциденти, у якому описано, які кроки необхідно вжити у разі порушення цілісності, доступності або конфіденційності інформаційних активів. [2]

Термін "кіберстійкість" є відносно свіжим, але стає все більш популярним і актуальним у галузі інформаційної та кібербезпеки. Він включає в себе ряд завдань і процесів, які відносяться до інформаційних технологій і захисту бренду. Кіберстійкість має ширший підхід, який охоплює здатність організації продовжувати ефективну роботу перед обличчям кіберзагроз і швидко відновлюватися після будь-яких збоїв або пошкоджень. Концепція

кіберстійкості визнає, що, незважаючи на найкращі заходи безпеки, порушення можуть і будуть відбуватися.

Кіберстійкість дозволяє підготуватися до атаки, забезпечує ефективну діяльність і протидію під час атаки, а також знижує можливі наслідки атаки на компанію. Кіберстійкість полягає в забезпеченні того, що бізнес процеси можуть і мають продовжуватися під час і після кіберінциденту.

Поняття кіберстійкості передбачає адаптацію до нових загроз і мінливого середовища. Це означає не лише захист від відомих загроз, але й можливість реагувати на нові та непередбачені виклики.[3]

Компанія, що заявляє про свою кіберстійкість, має надійні плани реагування на інциденти та відновлення після них. Це включає відновлення нормальної роботи систем і даних після атаки.

Кібербезпека та кіберстійкість — два терміни, які часто обговорюються в контексті захисту цифрових активів організації, але вони стосуються різних концепцій і підходів у сфері інформаційних технологій і безпеки.
Відмінності концепцій кібербезпеки та кіберстійкості показано на рис. 1.1.

Cyber Security	Cyber Resilience
Primarily focuses on prevention	Concentrates on adaptability and recovery
Utilises tools like firewalls, antivirus, and encryption	Uses strategies like incident response plans and backup systems
Aims to prevent breaches and unauthorised access	Aims to ensure continuity even after a breach
Addresses threats externally	Addresses threats both externally and internally, considering organisational resilience

Рис. 1. Різниця між кібербезпекою та кіберстійкістю

По суті, кібербезпека зосереджена на створенні бар’єрів, щоб не допустити зловмисників і захистити системи та дані від злому, використовує такі засоби як міжмережеві екрани, антивіруси, криптографію, спрямовує зусилля на запобігання порушенням безпеки і неавторизованому доступу, протидіє загрозам ззовні.

Натомість, кіберстійкість припускає, що системи можуть бути зламані, і підкреслює здатність працювати під час атаки та швидко відновлюватися після неї, концентрується на адаптивності і відновленні після порушень безпеки, використовує стратегії реагування на інциденти і системи резервного копіювання, спрямовує зусилля на забезпечення безперервності бізнесу навіть

після інциденту, протидіє загрозам як зовнішньо, так і внутрішньо, забезпечуючи організаційну стійкість.

Література

1. Cyber Threats and Advisories | Cybersecurity and Infrastructure Security Agency CISA. CISA. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories
2. Drolet M. Council Post: Eight Cybersecurity Trends To Watch For 2024. Forbes. URL: https://www.forbes.com/sites/forbestechcouncil/2023/12/26/eight-cybersecurity-trends-to-watch-for-2024/?sh=27023e5b4111The path to cyber resilience URL: https://www.greenbone.net/en/the-path-to-cyber-resilience/
3. Cyber_resilience – Wikipedia URL: https://en.wikipedia.org/wiki/Cyber_resilience