Додаток 14
Затверджено
Наказ Державного університету телекомунікацій
від «28 » березня 2022 р. № 31

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ ЗІ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА

на базі здобутого освітньо-кваліфікаційного рівня молодшого спеціаліста, освітньо-професійного ступеня фахового молодшого бакалавра, освітнього ступеня молодшого бакалавра
для здобуття першого (бакалаврського) рівня вищої освіти

Київ – 2022

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Мета вступного випробування — визначення рівня знань за напрямками професійної діяльності молодшого спеціаліста та формування контингенту студентів, найбільш здібних до успішного опанування дисциплін відповідної бакалаврської програми. Вступник повинен продемонструвати фундаментальні та професійно-орієнтовні знання та уміння, здатність вирішувати типові професійні завдання, передбачені програмою вступу.

Вимоги до здібностей і підготовленості абітурієнтів. Для успішного засвоєння освітньо-професійної програми бакалавра абітурієнти повинні мати базову середню спеціальну освіту з відповідної спеціальності та здібності до оволодіння знаннями, уміннями і навичками в галузі професійних наук.

Обов'язковою умовою є вільне володіння державною мовою.

Характеристика змісту програми. Програма вступного випробування має комплексний характер та складається із таких розділів професійних знань:

Розділ 1. Інформація та інформаційні технології.

Розділ 2. Кібербезпека інформаційно-комунікаційних систем.

Розділ 3. Технічні системи кіберзахисту.

Розділ 4. Управління у сфері кіберзахисту.

ПРОГРАМА ФАХОВОГО ВИПРОБУВАННЯ

РОЗДІЛ 1
ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Поняття інформації. Інформаційні процеси

Види та властивості інформації. Вимірювання інформації. Способи подання інформації. Системи числення. Основні форми подання інформації та її кодування в комп'ютері. Сучасні засоби зберігання та передавання інформації. Поняття інформаційної системи та їх класифікація. Основні інформаційні процеси.

Основи алгоритмізації та програмування

Інформаційна модель задачі. Поняття алгоритму. Властивості алгоритмів. Алгоритми з розгалуженням. Прості та складені умови у командах розгалуження. Циклічні алгоритми та їх опис. Цикли з передумовою та цикли з післяумовою. Циклічні алгоритми з покроковою зміною аргументів. Алгоритми-функції та алгоритми-процедури. Алгоритми пошуку. Алгоритми впорядкування. Загальні поняття складності алгоритмів.

Класифікація мов програмування. Об'єктна та структурна парадигми програмування. Основні поняття мови програмування: алфавіт, синтаксис і семантика. Основні елементи мови програмування: символи, слова, вирази та команди. Основні елементи конкретної мови програмування: алфавіт, операції, функції. Поняття програми. Системи програмування. Структура опису програми конкретною мовою програмування. Трансляція і відлагодження програм. Тестування програм.

Апаратне забезпечення інформаційних систем

Етапи розвитку обчислювальної техніки. Основні складові апаратної частини інформаційної системи. Основні характеристики ЕОМ. Функціональна схема та принципи функціонування комп'ютера. Запам'ятовувальні пристрої ЕОМ та їх основні характеристики. Мікропроцесор, його основні функції. Зовнішні пристрої ЕОМ, їх характеристики. Робота з дисками. Розміщення інформації на дисках. Магістрально-модульний принцип будови комп'ютера. Принципи роботи ЕОМ: програмного керування, адресності. Класифікація та основні характеристики сучасних комп'ютерів.

Програмне забезпечення інформаційних систем

Програмне забезпечення сучасних комп'ютерів. Класифікація програмного забезпечення. Прикладне програмне забезпечення комп'ютера. Операційна система комп'ютера, принципи роботи та функціонування. Основні функції операційної системи. Характеристики операційних систем. Основні команди операційних систем. Особливості операційної системи Windows. Правила роботи та основні команди.

Поняття файла, команди роботи з файлами. Каталоги та підкаталоги, команди операційної системи для роботи з каталогами. Архівація файлів, принципи роботи програм-архіваторів. Інсталяція та деінсталяція програмних засобів, суть процесів. Бази даних, їх призначення та класифікація. Типи баз даних. Призначення та основні типи запитів у базах даних. Пошук, впорядкування та фільтрування даних у сучасних базах даних. Системи керування базами даних, їх призначення та основні функції. Основи проектування баз даних та знань. Реляційні, ієрархічні та мережні бази даних, їх особливості та відмінності.

Текстовий редактор (призначення, основні функції, режими роботи, система команд). Редагування та форматування тексту в середовищі текстового редактора. Системи опрацювання графічних зображень. Графічний редактор, його призначення та основні функції. Електронні таблиці, їх призначення та основні функції. Режими роботи та система команд табличного процесора. Опрацювання табличних даних за допомогою електронних таблиць. Обчислення в середовищі електронних таблиць. Робота з функціями. Використання фільтрів. Побудова діаграм на основі табличних даних в середовищі табличного процесора. Поняття комп'ютерної презентації, її призначення, створення та демонстрація. Програми організації презентацій. Internet-браузери.

Комп'ютерні мережі

Комп'ютерні мережі. Класифікація та топологія. Основні апаратні засоби організації мереж. Програмні засоби комп'ютерних мереж. Глобальна мережа Інтернет, історія виникнення та принципи використання. Поняття та основні види мережених протоколів. Гіпертекстовий документ. Електронна пошта: принципи функціонування, способи використання програм, правила утворення електронної адреси. Телеконференції, їх класифікація та принципи роботи. Мобільний зв'язок, принципи функціонування. Основні принципи функціонування Bluetooth. Основні канали зв'язку та їх характеристики. Технологія World Wide Web гіпертекстових сторінок. Система адресації Internet. Поняття мови розмітки гіпертексту – мова HTML.

РОЗДІЛ 2.
КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Організація комп'ютерної безпеки та захисту особистих даних

Системи організації захисту комп'ютерних мереж. Програми безпеки комп'ютерних систем. Поняття комп'ютерних вірусів, їх класифікація. Антивірусні програми, принципи їх роботи. Комп'ютерна безпека та необхідність в її забезпеченні. Комп'ютерні віруси як основна загроза комп'ютерній безпеці. Основні види зловмисного ПЗ. Сучасний хакер, найпоширеніші вірусні загрози в Україні та їхні джерела. Основні симптоми зараження шкідливим ПЗ та рекомендації щодо забезпечення надійного захисту ПК.

Основні аспекти забезпечення безпеки мобільних пристроїв. Соціальна інженерія

Основні загрози та ризики безпеки мобільних пристроїв. Наслідки порушення безпеки мобільних пристроїв. Рекомендації щодо забезпечення захисту мобільних пристроїв (на базі Android та iOS). Поняття соціальної інженерії та її основні аспекти.

Поняття порушника інформаційної безпеки.

Умови та способи несанкціонованого доступу до конфіденційної інформації. Шляхи визначення джерел загроз інформаційній безпеці. Види загроз та основні типи порушень інформаційної безпеки. Світова мережа Інтернет: особливості побудови, можливі загрози. Організація безпечної роботи в мережі Інтернет.

РОЗДІЛ 3.
ТЕХНІЧНІ СИСТЕМИ КІБЕРЗАХИСТУ

Основи теорії кіл та сигналів в інформаційному та кіберпросторах

Основні електричні та магнітні величини. Поняття про електричне коло та його елементи. Класифікація елементів електричного кола. Загальні питання теорії кіл. Джерела електричної енергії та режими їх роботи. Електричні сигнали. Електричні кола постійного струму. Основні закони електричних кіл Електричні кола синусоїдного струму. Основні параметри синусоїдних струмів, напруг, електрорушійних сил. Методи розрахунку електричних кіл. Електричні фільтри. Чотириполюсники. Рівняння чотириполюсника. Методи визначення коефіцієнтів чотириполюсників. Симетричні та несиметричні чотириполюсники. Схеми заміщення чотириполюсників. Нелінійні електричні кола. Визначення робочих точок нелінійних елементів. Визначення реакції нелінійного елемента на зовнішні сигнали. Нелінійні елементи при гармонічному впливі.

Методи та засоби технічного захисту інформації

Технічний захист інформації і об'єкт захисту. Мета і завдання ТЗІ. Класифікація та характеристики технічних каналів витоку інформації. Причини створення акустичних каналів витоку інформації та методи акустичної розвідки. Проникнення інформаційних сигналів в лінії електроживлення та

заземлення. Електричні технічні канали витоку інформації. Прослуховування телефонних ліній. Методи і способи підключення до ліній зв'язку. Радіоканали витоку інформації та їх класифікація. Класифікація та характеристики візуально-оптичних каналів витоку інформації. Класифікація та характеристики матеріально-речових каналів витоку інформації. Основні методи закриття мовних сигналів у телефонних лініях. Поняття об'єкта інформаційної діяльності.

РОЗДІЛ 4.
УПРАВЛІННЯ У СФЕРІ КІБЕРЗАХИСТУ

Принципи управління інформаційною та кібербезпекою. Методи кіберзахисту.

Законодавство України з питань інформаційної та кібербезпеки. Інформаційні ресурси та інформаційна інфраструктура. Критична інформаційна інфраструктура. Сімейство стандартів ISO 27000.

Загрози інформаційній безпеці, кібербезпеці та їх джерела. Види вразливостей об'єктів кіберзахисту. Основні причини порушень інформаційної та кібербезпеки. Методи та види несанкціонованого доступу. Методи та технології запобігання та знешкодження загроз кібербезпеці.

Політика інформаційної та кібербезпеки. Верхній, середній та нижній рівні політики безпеки. Види організаційних документів у сфері інформаційної та кібербезпеки. Правила безпечного користування ІТКС.

Класифікація інформаційних ресурсів підприємства. Види інформації з обмеженим доступом.

Організаційні заходи з кібербезпеки, кіберзахисту. Робота з персоналом у сфері інформаційної та кібербезпеки. Робота з носіями конфіденційної інформації. Фізична безпека об'єктів кіберзахисту та засоби її забезпечення. Методи ідентифікації та аутентифікації. Управління доступом до об'єктів кіберзахисту.

Види інцидентів інформаційної та кібербезпеки. Аудит інформаційної та кібербезпеки.

Служба кібербезпеки (кіберзахисту) підприємства. Вимоги до фахівця з управління інформаційною та кібербезпекою. Економічне обґрунтування заходів кіберзахисту.

ЛІТЕРАТУРА

1. Ахрамович В.М., Чегренець В.М, Котенко А.М. Комп'ютерні мережі. Практикум / А95 В.М. Ахрамович, В.М. Чегренець, А.М. Котенко // Державний університет телекомунікацій. – К.: ДУТ, 2018. – 412 с. – 404 с.
2. Бурячок В.Л. , Толюпа С.В., Семко В.В., Бурячок Л.В., Складанний, П.М. Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Посібник. – К. : ДУТ - КНУ, 2016. – 178 с.

3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015.– 288 с
4. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Підручник. – К. : ТОВ «СІК груп Україна», 2015. – 449 с.
5. Голев Д. В., Русляченко О.Ю., Белова Ю.В., Гончарук Д.С. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 2 – Комплекси техничного захисту інформації Навч. посібник / За ред. чл.-кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 184.
6. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков — «Издательские решения», 2018. – 249 с.
7. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.
8. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.
9. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Частина1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев// За ред. ак. МАІ М.В. Захарченка.– Одеса: ОНАЗ ім. О.С. Попова, 2011. – 168 с.
10. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 - 216 с.
11. Іванченко С.О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
12. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем: підручник. К. ДУІКТ, 2010. – 316 с.
13. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: ХНЕУ, 2013. – 476 с..
14. Системи менеджменту інформаційної безпеки: Навчальний посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк. Львів: Видавництво Львівської політехніки, 2012. 232 с.
15. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: методичні рекомендації / Ю.О. Тихонов, В.О. Пшоннік // К.: ДУТ, 2018. – 54 с.
16. Управління інформаційною безпекою [Текст] : підручник: у 2 т. / Л. Ф. Єжова [та ін.]; Нац. авіац. ун-т. - Вид. 2-ге, допов. та перероб. - К.: НАУ, 2012. - Т.1. - 2012. - 369 с.

17. Управління інформаційною безпекою [Текст] : підручник : у 2 т. / Л. Ф. Єжова [та ін.]; Нац. авіац. ун-т. - Вид. 2-ге, допов. та перероб. - К.: НАУ, 2012. - Т.2. - 2012. - 347 с.
18. Bejtlich. R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response, 2013.
19. Krebs. B. Spam Nation: The Inside Story of Organized Cybercrime — from Global Epidemic to Your Front Door, 2014.

КРИТЕРІЇ ОЦІНЮВАННЯ

Рівень знань	Бали	Критерії оцінювання знань
Початковий	100-107	Абітурієнт має розповісти про місце та роль інформації в сучасному світі
	108-115	Абітурієнт називає властивості інформації; вибирає правильний варіант відповіді на рівні «так-ні»
	116-123	Абітурієнт двома-трьома словами має розповісти про об'єкти захисту інформації
Середній	124-132	Абітурієнт репродуктивно відтворює невелику частину навчального матеріалу, пояснюючи терміни у сфері захисту інформації
	133-141	Абітурієнт з допомогою викладача відтворює основний зміст навчальної теми, визначає основні заходи захисту інформації
	124-150	Абітурієнт самостійно відтворює фактичний матеріал теми, дає стислу характеристику системі захисту інформації
Достатній	151-159	Абітурієнт послідовно і логічно відтворює навчальний матеріал теми, виявляє розуміння термінології, характеризує технічні засоби захисту інформації
	160-168	Абітурієнт володіє навчальним матеріалом і використовує знання за аналогією, дає правильні визначення, аналізує можливі загрози інформації, визначає причинно-наслідкові зв'язки між ними
	169-177	Абітурієнт оперує навчальним матеріалом, формує нескладні висновки, обґрунтовуючи їх конкретними фактами; самостійно встановлює причинно-наслідкові зв'язки між вразливостями та загрозами інформації
Високий	178-185	Абітурієнт використовує набуті знання для вирішення нової навчальної проблеми; виявляє розуміння системи захисту інформації; робить аргументовані висновки, спираючись на широку джерельну базу

	168-193	Абітурієнт володіє глибокими знаннями, може вільно та аргументовано висловлювати власні судження щодо розробки основних документів з питань захисту інформації
	194-200	Абітурієнт системно володіє навчальним матеріалом; виявляє особисту позицію щодо розробки системи захисту інформації організації; уміє відокремити проблему і визначити шляхи її розв'язання; користується джерелами інформації, аналізує та узагальнює їх.

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Склад фахової екзаменаційної комісії визначається наказом ректора Державного університету телекомунікацій від 22.02.2022 р. № 26 «Про утворення підрозділів Приймальної комісії», робота комісії та порядок проведення вступного випробування регламентуються «Положенням про Приймальну комісію» введеного в дію наказом № 35 від 10 травня 2022 року.

Голова фахової екзаменаційної комісії Г.І. Гайдур