ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____ В.В. Семенець
«28» 02 2019 р.

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
для вступу на освітній ступінь магістра

Спеціальність 125 Кібербезпека

Освітня програма: Адміністративний менеджмент у сфері захисту інформації

Протокол засідання приймальної комісії
№ 14 від 28.02 2019 р.

Голова фахової
атестаційної комісії _____ О.В. Лемешко
(підпис, ініціали, прізвище)

Відповідальний секретар
приймальної комісії _____ А.В.Снігуров
(підпис, ініціали, прізвище)

Харків 2019

Програму схвалено на засіданні Вченої ради факультету ІК
Протокол №4 від 14.02.2019р.
Декан ф-ту ІК А.В.Снігуров

«__»_____ 2019р.

НАВЧАЛЬНІ ДИСЦИПЛІНИ, ТЕМАТИКА ТА НАВЧАЛЬНА ЛІТЕРАТУРА

1. ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

Теми:

1.1. Акустичні канали витоку інформації. Методи та засоби захисту мовної інформації й оцінка їх ефективності

1.2. Побічні електромагнітні випромінювання наводки (ПЕВМН) технічних засобів передачі, зберігання та обробки інформації. Методи і засоби захисту ТСПІ при витоку інформації через ПЕВМН.

1.3. Оптичні канали витоку інформації. Методи і засоби захисту інформації при витоку її через оптичні канали.

Навчальна література:

1. Технические средства и методы защиты информации /Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Под. Ред. Зайцева А.П. – 4-е изд. М.: Горячая линия – Телеком, 2009. – 616 с.

2. Инженерно-техническая защита информации: учебное пособие/ Торокин А.А. – М.: Гелиос АРВ, 2005. – 960 с.

2. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Теми:

2.1. Система міжнародних стандартів ISO27к. Область застосування стандартів. Зміст процесу впровадження створення систем менеджменту інформаційної безпеки (СМІБ). Життєвий цикл СМІБ. Вплив процесу управління інформаційною безпекою на інші процеси установи (організації, підприємства).

2.2. Поняття ризику, кількісне визначення величини ризику, якісне визначення величини ризику. Процесна модель управління ризиками. Способи обробки ризиків: прийняття ризику, зменшення ризику, передача ризику, ухід від ризику. Визначення системи управління інформаційними ризиками. Структура документації по управлінню ризиками. Процеси управління ризиками.

2.3. Основні етапи створення СМІБ згідно стандарту ISO/IEC 27001:2013. Політика СМІБ: цілі, зміст, перегляд. Основні етапи

впровадження і функціонування СМІБ. Вимоги до документації. Управління інцидентами, пов'язаними з забезпечення безпеки інформації. Управління безперервністю бізнесу. Організаційні основи управління інцидентами. Зміст процесу управління інцидентами. Зміст процесу управління безперервністю бізнесу. Методи підтримки процесу безперервністю бізнесу.

2.4. Основи оцінки та управління ризиками інформаційної безпеки

2.5. Інструментальні засоби управління ризиками інформаційної безпеки

Навчальна література:

1. Астахов А.А. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.

2. Міжнародний стандарт: ISO/IEC 27000:2016 Information technology. Security techniques. Information security management systems . Overview and vocabulary.

3. Міжнародний стандарт: ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements.

4. Міжнародний стандарт: ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls.

5. Міжнародний стандарт: ISO/IEC 27003:2010 Information technology. Security techniques. Information security management system implementation guidance.

6. Міжнародний стандарт: ISO/IEC 27004:2009 Information technology. Security techniques. Information security management. Measurement.

7. Міжнародний стандарт: ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management.

3. ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Теми:

1. Основні положення про побудову стійких шифрів.
2. Методи побудови симетричних систем.
3. Криптосистеми зі змінною структурою

4. Методи побудови асиметричних систем.

5. Генератори випадкових та псевдо випадкових послідовностей чисел.

6. Конструкції геш-функцій та алгоритмів видобутку криптографічних контрольних сум.

7. Механізм електронного цифрового підпису.

8. Конструкції потокових шифрів.

9. Криптографічні протоколи.

Навчальна література:

1. Поповський В.В., Персіков А.В. Захист інформації в телекомунікаційних системах. Том 1: Підручник. – СМИТ, 2006. – 238 с.

2. Поповський В.В., Персіков А.В. Захист інформації в телекомунікаційних системах. Том 2: Підручник. – СМИТ, 2006. – 292 с.

3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

4. БЕЗПЕКА ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Теми:

4.1. Принципи побудови та функціонування сучасних операційних систем, що використовуються в інформаційно-комунікаційних системах. призначення, функції та архітектура операційних систем. архітектура операційних систем. організація обчислювального процесу в операційних системах. управління процесами та потоками. поняття дескриптору та контексту процесу. управління пам'яттю. методи, алгоритми та засоби. файлові системи. організація файлів та доступ до них. фізична організація файлової системи. контроль доступу до файлів.

4.2. Механізми забезпечення безпеки ресурсів операційних систем за допомогою вбудованих механізмів. облікові записи користувачів, групи та безпека входу у систему. дескриптори та маркери процесів. типи облікових записів в операційних системах. порядок створення та управління обліковими записами. групові облікові записи. групова політика об'єктів.

4.3. Призначення служби каталогів в інформаційно-комунікаційних системах. архітектура active directory. планування розгортання active

directory. компоненти доменних служб active directory, типи облікових записів, реалізованих в active directory та стратегія їх управлінням. планування групової політики. сайти та реплікація в active directory.

Навчальна література:

1. Бондаренко, М. Ф. Операційні системи : навч. посібник / М. Ф. Бондаренко, О. Г. Качко. – Х. : Компанія СМІТ, 2008. – 432 с.

2. Матвієнко, М. П. Архітектура комп'ютера : навч. посіб. / М. П. Матвієнко, В. П. Розен, О. М. Закладний ; МОНМС України. – К. : Ліра-К, 2013. – 264 с. : іл. – МОН України.

3. Поповский, В. В. Основы криптографической защиты информации в телекоммуникационных системах : [учеб. изд.]. Ч.1 / В. В. Поповский, А. В. Персиков. – Х. : СМИТ, 2010. – 352 с.

4. Поповский, В. В. Основы криптографической защиты информации в телекоммуникационных системах : [учеб. изд.]. Ч.2 / В. В. Поповский, А. В. Персиков. – Х. : СМИТ, 2010. – 296 с.

5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – М.-СПб. : Питер, 2012. – 944 с. (Учебник для вузов).

5. ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Теми навчальної дисципліни:

1. Правові основи організації спеціального діловодства. Класифікація конфіденційної інформації. Законодавство України щодо захисту конфіденційної інформації. Основні положення закону України “Про державну таємницю”.

2. Порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію.

3. Порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять державну таємницю та конфіденційну інформацію

Навчальна література:

1. Організація конфіденційного діловодства / С. М. Головань, О. М. Новіков, В. В. Поповський, В. О. Хорошко. – К., 2007

2. Замула, О. А. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації : навч. посіб. / О. А. Замула, Ю. І. Горбенко, О. І. Шумов ; МОН України, Харк. нац. ун-т радіоелектроніки. – Х. : ХНУРЕ, 2010. – 248 с.

3. Палеха, Ю. І. Загальне документознавство : навч. посібник / Ю. І. Палеха, Н. О. Леміш. - 2-ге вид., - К. : Лра-К, 2009. – 434 с.

4. Правові основи захисту інформації з обмеженим доступом. Курс лекцій. Марущак А.І. - К.: КНТ, 2007. -208с.

5. Закон України „ Про інформацію " .

6. Закон України „ Про державну таємницю" .

7. Постанова Кабінету Міністрів України „ Про затвердження інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, що є власністю держави ".

2. ПОРЯДОК ПРОВЕДЕННЯ БЛАНКОВОГО ТЕСТУВАННЯ

Загальна кількість завдань в тесті – 120. Кількість визначених дисциплін – 5.

Тест для кожної дисципліни складається з двох тем (теорії та практики).

Кількість варіантів відповідей у кожному тестовому завданні – 5.

Бланк тестування складається з 30 завдань, кількість варіантів бланків–4.

Тривалість проведення фахового випробування складає 120 хвилин.

Тематична розбивка тесту: 5 тем з теоретичними завданнями (72 завдання) і 5 тем із практичними завданнями (28 завдань). Усього в тесті 120 завдань.

1. Тема 1. Основи технічного захисту інформації – 24 завдання.
2. Тема 2. Менеджмент інформаційної безпеки – 12 завдань.
3. Тема 3. Основи криптографічного захисту інформації – 20 завдань.
4. Тема 4. Безпека інформаційно-комунікаційних систем – 24 завдання.

5. Тема 5. Основи національної безпеки – 12 завдань.

6. Практика 1. Основи технічного захисту інформації – 8 завдань
7. Практика 2. Менеджмент інформаційної безпеки – 4 завдання
8. Практика 3. Основи криптографічного захисту інформації – 4 завдання
9. Практика 4. Безпека інформаційно-комунікаційних систем – 8 завдань
10. Практика 5. Основи національної безпеки – 4 завдання