ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____ В.В. Семенець
«04» 02. 2020 р.

ПРОГРАМА
ДОДАТКОВОГО ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
для вступу на освітній ступінь магістра

Спеціальність 125 Кібербезпека

Освітні програми:
1. Безпека інформаційних і комунікаційних систем.
2. Безпека державних інформаційних ресурсів.
3. Адміністративний менеджмент у сфері захисту інформації.
4. Системи технічного захисту інформації, автоматизація її обробки

Протокол засідання приймальної комісії
№ 8 від 04.02. 2020 р.

Керівник проектної
групи _____ В.І. Руженцев
(підпис, ініціали, прізвище)

Відповідальний секретар
приймальної комісії _____ Є.П.Федоренко
(підпис, ініціали, прізвище)

Харків 2020

1. НАВЧАЛЬНІ ДИСЦИПЛІНИ, ТЕМАТИКА ТА НАВЧАЛЬНА ЛІТЕРАТУРА

1. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Теми навчальної дисципліни:

3.1 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).

3.2 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.

3.3 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.

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.

2. ОСНОВИ ТЕОРІЇ КІЛ, СИГНАЛІВ ТА ПРОЦЕСІВ

Теми навчальної дисципліни:

1. Основні поняття та елементи електричних кіл.
2. Основні закони і методи розрахунку кіл.
3. Режим синусоїдних коливань в електричних колах.
4. Частотні характеристики електричних кіл.
5. Класифікація та математичні моделі сигналів та процесів;
6. Сингулярні функції та їх використання при моделюванні детермінованих сигналів;
7. Гармонічний аналіз періодичних сигналів;
8. Спектральний аналіз неперіодичних сигналів;
9. Дискретні сигнали та методи їх аналізу;
10. Проходження детермінованих сигналів через лінійні кола з постійними параметрами.

Теоретичні завдання: *Основні закони та методи аналізу кіл.Змінний і синусоїдний струм та їхні основні параметри. Комплексна амплітуда. Явище резонансу в одиночних контурах. Класичний метод аналізу перехідних процесів. Основні поняття та означення. Часовий метод аналізу перехідних процесів. Часові характеристики.*

Навчальна література:

1.Основи теорії кіл, сигналів та процесів в СТЗІ [Текст]: Підручник для студентів ВНЗ Ч.1. / Ю.О. Коваль, І.О. Милютченко, А.М. Олейніков, В.М. Шокало та ін; за заг. редакцією В.М. Шокала. – Харків: НТМТ, 2011. – 544 с.

2. Коваль Ю.О., Ликова Г.О., Милютченко І.О. Задачник з основ теорії електро-радіокіл: Навч. посібник для студентів ВНЗ. Харків: ХНУРЕ; 2010. 196 с.

3. Гоноровский И.С. Радиотехнические цепи и сигналы: Учебник. – М.: Радио и связь, 1986. – 512 с.

4. Баскаков С.И. Радиотехнические цепи и сигналы. Учебник. – 2-е изд. – М.: Высшая школа, 1988. – 448 с.

5. Радиотехнические цепи и сигналы. Учеб. пособие для вузов / Под ред. К.А. Самойло. – М.: Радио и связь, 1982. – 528 с.

6. Радиотехнические цепи и сигналы: Примеры и задачи / Под ред. И.С. Гоноровского. – М.: Радио и связь, 1989. – 128 с.

3. КОМПЛЕКСИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Теми навчальної дисципліни:

1. Основні поняття про інформацію як предмет захисту. Види, джерела та носії інформації, що підлягає захисту. Об'єкти інформаційної діяльності (ОІД), їх структура.

2. Технічні канали витоку інформації (ТКВІ), визначення, їх структура та класифікація

3. Технічні канали витоку інформації, що обробляється технічними засобами.

3.1. Побічні електромагнітні випромінювання (ПЕМВ).

3.4. Наведення побічних електромагнітних полів на випадкові антени (ПЕМН).

4. Технічні канали витоку інформації, що озвучується на ОІД.

4.1. Аналогові сигнали, їх спектри.

4.2. Спрямовані мікрофони.

4.3. Вібраційні канали витоку інформації.

4.4. Закладні пристрої.

4.5. Акустоелектричні перетворювачі.

4.6. Лазерні засоби акустичної розвідки.

5. Технічні канали витоку інформації, що візуалізується на ОІД.

Видова розвідка, її основні характеристики та можливості.

6. Методи технічного захисту інформації.

6.1. Класифікація заходів та засобів ТЗІ.

6.2. Пасивні засоби ТЗІ.

6.3. Активні засоби ТЗІ.

6.4. Організаційні заходи ТЗІ.

7. Захист інформації, що обробляється технічними засобами.

7.1. Екранування ПЕМВ.

7.2. Фільтри небезпечних сигналів.

7.3. Активний захист ПЕМВ і наводок.

8. Захист інформації, що озвучується на ОІД.

8.1. Звукоізоляція виділених приміщень.

8.2. Активний захист мовної інформації.

8.3. Виявлення закладних пристроїв.

9. Захист інформації, що візуалізується на ОІД.

Методи і засоби захисту видової інформації.

Навчальна література:

1. Олейніков А.М. «Методи та засоби захисту інформації» Навчальний посібник для студентів вищих навчальних закладів // Харків: НТМТ , 2014. – 298с

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

3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Киев: Изд-во «Юниор».2003.– 504 с

4. Хорев А.А. Способы и средства защиты информации. – М.: МО РФ, 2000.– 316 с.

4. МЕТРОЛОГІЯ ТА ВИМІРЮВАННЯ

Теми навчальної дисципліни:

1. Міжнародна система одиниць СІ, одиниці величин в електрорадіотехніці.
2. Класифікація похибок.
3. Обробка результатів прямих, непрямих, сумісних та сукупних вимірювань.
4. Метрологічна атестація, повірка, калібрування.
5. Принципи дії аналогових та цифрових аналізаторів спектра.
6. Вимірювачі параметрів кіл R,L,C добротності, АЧХ.
7. Принципи дії аналогових та цифрових аналізаторів спектра.
8. Вимірювання змінної та ВЧ напруги.

Навчальна література:

1 Кукуш В.Д. Электрорадиоизмерения / Учеб. пособие для вузов. – М.: Радио и связь, 1985.

2 Дворяшин Б.В. Метрология и радиоизмерения / Учеб. пособие для студ. высш. учеб. заведений.– М.: Издательский центр «Академия», 2005.

3 Методичні вказівки до всіх видів занять з дисципліни „Метрологія та вимірювання” для студентів денної форми навчання з напряму 1601 “Інформаційна безпека” / Упоряд.: В.Б. Бєлявцев, В.Г.Лихограй – ХНУРЕ, 2007.

5. ТЕХНІЧНІ ЗАСОБИ ОХОРОНИ ОБ'ЄКТІВ

Теми навчальної дисципліни:

1. Оптичні засоби виявлення. Основні характеристики оптичних засобів виявлення порушника.
2. Методи підвищення завадостійкості пасивних ІЧ засобів виявлення порушників.
3. Системи і засоби контролю доступу, особливості їх застосування. Ідентифікаційні карти і їх структурні схеми.
4. Радіохвольові і радіопроменеві засоби виявлення. Структурні схеми мікрохвольових давачів і допплерівських давачів руху.
5. Конструкції чутливих елементів засобів виявлення (ємнісний давач, давач Холла, вимірювальна схема на основі моста опорів постійного струму).

Навчальна література:

1. Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. – М.: Горячая линия Телеком, 2004. – 367 с.
2. Дж. Фрайден. Современные датчики. Справочник. Техносфера. – М., 2005.

6. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Теми навчальної дисципліни:

1. Основні поняття організаційного забезпечення технічного захисту інформації
2. Особливості роботи з персоналом, який володіє конфіденційною таємницею.
3. Перевірки стану системи ТЗІ.
4. Вартісні залежності захисту інформації.
5. Розподіл ймовірностей виникнення загроз безпеці інформації в інформаційній системі.

Навчальна література:

1. Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. — М.: Гелиос АРВ, 2005. – 192 с.

2. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. – М.: ИНФРА-М, 2001. – 304 с.

3. Малюк А.А. Информационная безопасность: Учебное пособие. – М., 2004. – 208 с.

4. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.

5. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навч. посібник.– К.: Вид-во Європ. ун-ту, 2006. – 102 с.

7. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Теми навчальної дисципліни:

1 Симетричні криптографічні системи

2 Асиметричні криптографічні системи

3 Методи автентифікації інформації

4 Цифровий підпис та його властивості

5 Криптографічні протоколи

Навчальна література:

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 868 с.

2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2012 р.

8. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Теми навчальної дисципліни:

1. Архітектура комп'ютерних систем. Рівень архітектури набору команд. Загальний огляд рівня архітектури набору команд. Типи даннях. Формати команд. Адресація. Основні цифрові логічні схеми. Пам'ять.

2. Програмне забезпечення. Структура програмного забезпечення. Архітектура, призначення і функції операційних систем.

3. Засоби налагодження програмного забезпечення. Надійність програмного забезпечення. Методологія діагностування програмного забезпечення.

4. Архітектура та програмне забезпечення комп'ютерних мереж. Базові топології та протоколи комп'ютерної мережі. Технологія TCP/IP. Принципи об'єднання мереж. Технології забезпечення безпеки мереж. Ідентифікація і автентифікація даних і джерел даних. Особливості функціонування міжмережевих екранів. Основні схеми мережевого захисту на базі міжмережевих екранів.

Навчальна література:

1. Таненбаум Э. Архитектура компьютера. 5-е изд. – СПб.: Питер, 2007. – 844 с.

2. Таненбаум Э. Современные операционные системы. 3-е изд. – СПб.: Питер, 2010. – 1120 с.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологи, протоколы: Ученик для вузов – СПб.: Питер, 2006 – 958 с.

9. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Теми навчальної дисципліни:

1. Безпека прикладного рівня. Протокол SSL/TLS. Криптографія в SSL/TLS. Автентифікація в протоколі HTTP. Безпека протоколу FTP.

2. Сторонні протоколи. Автентифікація X509. Сервер автентифікації Kerberos.

3. Допоміжні протоколи. Протокол SNMP.

4. 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.

5. 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.

6. 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. Горбенко І. Д., Гріненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004 – 368 с.

2. Грайворонський М.В., Новіков О.М. Безпека інформаційно- комунікаційних систем. Підручник. – К:Видавнича група BHV, 2009.-608 с.

3. Вильям Столлингс. Основы защиты сетей. Приложения и стандарты. М.:Вильямс, 2002. – 432 с.

4.Ричард Э. Смит. Аутентификация: от паролей до открытых ключей. — М.: Вильямс, 2002. — 415 с.

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

6. 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.

10. НОРМАТИВНО ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Теми навчальної дисципліни:

1. Законодавство України у галузі інформаційної безпеки та захисту інформації з обмеженим доступом. Місце та роль захисту інформації в системі національної безпеки України. Принципи забезпечення безпеки інформації в інформаційно – телекомунікаційних системах. Моделі загроз інформаційної безпеки. Мета та задачі захисту інформації в інформаційно – телекомунікаційних системах. Міжнародні стандарти та нормативні документи України в галузі захисту інформації. Загальні питання доступу до інформації та відповідальність за порушення законодавства про інформацію.

2. Напрями державної політики України в інформаційній сфері. Правові основи захисту інформації. Поняття, правові ознаки та види інформації. Правовий статус інформації як об'єкта цивільних прав. Зміст суб'єктивного права на інформацію. Інформація – як об'єкт захисту. Захист інтелектуальної власності.

Навчальна література:

1. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010 - 11 с.

2. Замула О.А. Захист держаних секретів. Навчальний посібник. ХНУРЕ – 2003. – 206 с.

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

4. 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.

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

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

7. Закон України „ Про інформацію " .

8. Закон України „ Про державну таємницю" .

9. 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 – 36.

Тестування складається з 12 завдань, кількість варіантів бланків – 3.

Час на проведення тестування – 60 хвилин.

Оцінка «склав» виставляється у випадку 5 та більше правильних відповідей на завдання тесту. Це відповідає оцінці «задовільно» 12-бальної шкали оцінювання, яка використовується у середній школі. Оцінка «не склав» виставляється вступнику у випадку 4 та менше правильних відповідей на завдання тесту.