ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____В.В. Семенець
«15» 04 2020 р.

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
для вступу на другий (магістерський) рівень вищої освіти

Спеціальність 125 Кібербезпека

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

Протокол засідання приймальної комісії

№ 25 від 15.04 2020 р.

Голова фахової комісії _____ Г.З. Халімов

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

Харків 2020

НАВЧАЛЬНІ ДИСЦИПЛІНИ, ТЕМАТИКА ТА НАВЧАЛЬНА ЛІТЕРАТУРА

1. КОМПЛЕКСИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

Теми навчальної дисципліни:

1. Види, джерела та носії інформації, що підлягає захисту. Об'єкти інформаційної діяльності (ОІД), їх структура.

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

3. Технічні канали витоку інформації, що обробляється технічними засобами

3.1. Побічні електромагнітні випромінювання (ПЕМВ).

3.2. Перехоплення ПЕМВ.

3.3. Наведення побічних електромагнітних полів на випадкові антени (ПЕМН) та їх перехоплення.

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

4.1. Аналогові мовні 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.

6.5. Показники та норми ефективності ТЗІ.

7. Захист інформації, що обробляється технічними засобами.

7.1. Екранування ПЕМВ.

7.2. Фільтри небезпечних сигналів.

7.3. Активний захист ПЕМВ.

8. Захист інформації, що озвучується на ОІД.

8.1. Приховування акустичних інформативних сигналів. 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.

5. Олейніков А.М., Коваль В.П. Захист мовної інформації методом радіомоніторингу: Навч. посібник – Харків: ХНУРЕ, 2007. – 96 с.

6. 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. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Теми навчальної дисципліни::

1.1. 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).

1.2. 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.

1.3. 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. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ.

Теми навчальної дисципліни:

1. Безпека прикладного рівня.

1.1 Протокол SSL/TLS. Загальна архітектура. Протокол записів. Протокол помилок.

1.2 Протокол SSL/TLS. Протокол узгодження параметрів. Криптографія в SSL/TLS.

1.3 Безпека системи електронної пошти.

1.4 Автентифікація в протоколі HTTP.

1.5 Архітектура протоколу SSH. Транспортний протокол.

1.6 Архітектура протоколу SSH. Протокол автентифікації і протокол з'єднань.

1.7 Безпека протоколу FTP.

2. Сторонні протоколи.

2.1 Автентифікація X509.

2.2 Сервер автентифікації Kerberos.

2.2 ASN/1.

2.3 Протокол LDAP. Інформаційна модель.

2.4 Протокол LDAP. Функціональна модель.

2.5 Протокол LDAP. Автентифікація в LDAP.

3. Допоміжні протоколи.

3.1 Протокол SNMP. Загальні поняття і архітектура.

3.2 Протокол SNMP. Модель безпеки.

3.3 Безпека протоколів віддаленого доступу (CHAP, RADIUS)

4. Принципи побудови та функціонування сучасних операційних систем, що використовуються в інформаційно-комунікаційних системах.

4.1. 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.

5. 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.

7. 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).

4. 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. Аналіз перехідних процесів класичним методом.
6. Часовий метод аналізу перехідних процесів.
7. Класифікація та математичні моделі сигналів та процесів;
8. Сингулярні функції та їх використання при моделюванні детермінованих сигналів;
9. Гармонічний аналіз періодичних сигналів;
10. Спектральний аналіз неперіодичних сигналів;
11. Дискретні сигнали та методи їх аналізу;
12. Вузькосмугові сигнали;
13. Модульовані сигнали;
14. Проходження детермінованих сигналів через лінійні кола з постійними параметрами;
15.Перетворення сигналів у нелінійних радіотехнічних колах.

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. Часовий метод аналізу перехідних процесів. Часові характеристики.

Практичні завдання: Закони Ома та Кірхгофа в комплексній формі. Послідовне та паралельне увімкнення елементів R, L, C. Комплексні вхідні та передатні функції кола. АЧХ, ФЧХ. Розрахунок сталої часу в R, C і R, L колах. Розрахунок перехідних процесів у розгалужених R, C і R, L колах при дії джерела постійної ЕРС. Розрахунок простого кола з одним джерелом постійної напруги.

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.

5. 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.
9. Електромеханічні вимірювальні перетворювачі.
10. Робочі засоби вимірювання постійної напруги і опору.
11. Засоби вимірювання параметрів модульованих коливань.
12. Електроннолічильні частотоміри.

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.

6. 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. Застосування технічних засобів спостереження для контролю території. Технічні параметри телевізійних камер стеження.

4. 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.

7. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

Теми навчальної дисципліни:

1. Особливості роботи з персоналом, який володіє конфіденційною таємницею.
2. Об'єкти категоріювання.
3. Атестація комплексів технічного захисту інформації.
4. Перевірки стану системи ТЗІ.
5. Вартісні залежності захисту інформації.
6. Розподіл ймовірностей виникнення загроз безпеці інформації в інформаційній системі.
7. Оцінка захищеності інформаційної системи.

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.

8. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.

Теми навчальної дисципліни:

1 Математичні основи криптології

1.1 Теорія чисел та груп, скінченні поля Галуа, особливості застосування в криптографії.

1.2 Еліптичні та гіпереліптичні групи, основи застосування в криптографії.

1.3 Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.

2 Симетричні криптографічні системи

2.1 Основи теорії секретних систем (конфіденційності).

2.2 Симетричні криптографічні перетворення та їх властивості.

2.3 Джерела ключів та ключової інформації, вимоги до них.

3 Асиметричні криптографічні системи

3.1 Вступ в теорію асиметричних крипто перетворень.

3.2 Асиметричні крипто перетворення в групах точок еліптичних кривих.

3.3 Джерела ключів асиметричних криптосистем та вимоги до них.

4 Методи автентифікації інформації

4.1 Методи та механізми автентифікації в криптосистемах.

4.2 Методи та механізми захисту від несанкціонованого доступу.

4.3 Методи та механізми імітозахисту в радіосистемах.

5 Цифровий підпис та його властивості

5.1 Електронні цифрові підписи з додатком.

5.2 Електронні цифрові підписи з відновлення повідомлень.

5.3 Властивості та основи застосування електронних цифрових підписів

6 Криптографічні протоколи

6.1 Криптографічні механізми та протоколи управління ключами.

6.2 Криптографічні механізми та протоколи автентифікації.

6.3 Синтез та аналіз криптографічних протоколів.

6.4 Квантова криптографія та крипто аналіз.

7 Криптографічний аналіз асиметричних криптосистем

7.1 Вступ в теорію та практику крипто аналізу.

7.2 Методи крипто аналізу асиметричних криптосистем.

7.3 Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих.

8 Криптографічний аналіз симетричних криптосистем

8.1 Вступ в теорію крипто аналізу в симетричних криптосистемах.

8.2 Методи крипто аналізу блокових симетричних криптосистем.

8.3 Методи крипто аналізу потокових симетричних криптосистем.

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.

9. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ.

Теми навчальної дисципліни:

1. Архітектура комп'ютерних систем

1.1. Архітектура комп'ютерної системи. Функціонування комп'ютерної системи. Обробка переривань. Архітектура введення-виведення. Таблиця стану пристроїв. Прямий доступ до пам'яті. Структура пам'яті. Апаратний захист пам'яті і процесора. Апаратний захист адрес пам'яті в системах з теговой архітектурою. Організація апаратного захисту пам'яті і процесора.

1.2. Цифровий логічний рівень. Основні цифрові логічні схеми. Пам'ять. Мікросхеми процесорів і шини. Приклади центральних процесорів. Приклади шин. Інтерфейси.

1.3. Рівень мікроархітектури. Приклад мікроархітектури. Розробка рівня мікроархітектури. Підвищення продуктивності.

1.4. Рівень архітектури набору команд. Загальний огляд рівня архітектури набору команд. Типи даннях. Формати команд. Адресація.

2. Програмне забезпечення

2.1. Структура програмного забезпечення. Архітектура, призначення і функції операційних систем.

2.2. Прикладне програмне забезпечення для операційних систем: пакети прикладних програм MS Office.

2.3. Інформаційні технології та спеціалізовані засоби моделювання. Програмні пакети Mathcad, SMath Studio.

2.4. Програмні пакети Mathlab, SciLab.

2.5. Моделювання в системі SIMULINK.

3. Засоби налагодження програмного забезпечення

3.1. Надійність програмного забезпечення. Методологія діагностування програмного забезпечення.

3.2. Тестування модулів. Інтеграція модулів, тестування зовнішніх функцій і комплексів програм. Модернізація програмного забезпечення.

4. Архітектура та програмне забезпечення комп'ютерних мереж

4.1. Архітектури комп'ютерних мереж. Еталонні моделі взаємодії систем. Загальна архітектура мережі NGN. Базові топології та протоколи комп'ютерної мережі. Системи автоматизованого проектування комп'ютерних мереж.

4.2. Технології фізичного та канального рівнів. Характеристики ліній передачі даних на основі різних середовищ. Методи множинного доступу до каналу передачі даннях. Базові технології управління доступом до каналу передачі даних.

4.3. Базові мережеві технології. Технологія TCP/IP. Принципи об'єднання мереж.

4.4. Технології забезпечення безпеки мереж. Ідентифікація і автентифікація даних і джерел даних. Особливості функціонування міжмережевих екранів. Основні схеми мережевого захисту на базі міжмережевих екранів.

4.5. Побудова віртуальних приватних мереж(VPN) на базі технології MPLS. Послуги якості обслуговування. Топологія мережі доступу MPLS - VPN. VPN Solutions Center(центр рішень VPN).

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.

10. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Теми навчальної дисципліни:

1. Законодавство України у галузі інформаційної безпеки та захисту інформації з обмеженим доступом.

1.1 Місце та роль захисту інформації в системі національної безпеки України. Національна безпека України та її складові частини. Державна політика у сфері

інформаційної безпеки. Поняття і зміст інформаційної безпеки України. Загрози національним інтересам в інформаційній сфері.

1.2 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. Розробка Концепції забезпечення інформаційної безпеки організації. Розробка корпоративної політики забезпечення інформаційної безпеки організації.

1.3 Правовий режим захисту державної таємниці.

Проблемні питання у сфері захисту інформаційних ресурсів, віднесених до державної таємниці, та шляхи їх вирішення. Загальні питання доступу до інформації та відповідальність за порушення законодавства про інформацію. Державна таємниця та система її охорони. Віднесення інформації до державної таємниці. Засекречування та розсекречування матеріальних носіїв інформації. Режимно-секретні органи. Допуск громадян до державної таємниці. Доступ громадян до державної таємниці. Обов'язки громадянина щодо збереження державної таємниці. Контроль за забезпеченням охорони державної таємниці. Відповідальність за порушення законодавства про державну таємницю.

2. Напрями державної політики України в інформаційній сфері.

2.1 Ліцензійна та сертифікаційна діяльність у галузі захисту інформації. Законодавство України про ліцензування видів господарчої діяльності. Сертифікація засобів технічного захисту інформації. Правова регламентація охоронної діяльності.

2.2 Особливості сучасного етапу розвитку інформаційних технологій та їх вплив на безпеку інформації. Правові основи захисту інформації із застосування технічних засобів. Правовий статус 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. Злочини у сфері комп'ютерної інформації. Міжнародне законодавство у галузі захисту інформації.

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 - 15 с.

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

2. ПОРЯДОК ПРОВЕДЕННЯ БЛАНКОВОГО ТЕСТУВАННЯ

Загальна кількість завдань в тесті – 120.
Тест для кожної дисципліни складається 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.