ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____ В.В. Семенець
«18» ____02____ 2021 р.

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
для вступу на освітній ступінь магістра

Спеціальність __125 Кібербезпека_____

Протокол засідання приймальної комісії
№ 12 від 18.02. 2021 р.

Голова фахової комісії _____Г.З. Халімов
(підпис, ініціали, прізвище)

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

Харків 2021

НАВЧАЛЬНІ ДИСЦИПЛІНИ, ТЕМАТИКА ТА НАВЧАЛЬНА ЛІТЕРАТУРА

1. БЕЗПЕКА 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).

2. ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ 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.

3. ОСНОВИ 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. Радіоелектроний канал витоку інформації

3.1. Побічні електромагнітні випромінювання (ПЕМВ).

3.2. Перехоплення ПЕМВ.

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

4. Вібро-акустичний канал витоку інформації

4.1. Аналогові мовні сигнали, їх спектри

4.2. Спрямовані мікрофони.

4.3. Вібраційні канали витоку інформації.

4.4. Закладні пристрої (акустичні, радіоакустичні, для телефонних ліній).

4.5. Акустоелектричні перетворювачі.

4.6. Лазерні системи акустичної розвідки..

5.Візуально-оптичний канал витоку інформації

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.

6.5. Показники та норми ефективності ТЗІ.

7. Захист інформації від витоку по радіоелектроному каналу

7.1. Екранування ПЕМВ.

7.2. Фільтри небезпечних сигналів.

7.3. Активний захист ПЕМВ.

7.4. Захист інформації в телефонних лініях

8. Захист інформації від витоку по вібро-акустичному каналу

8.1. Приховування акустичних інформативних сигналів. Звукоізоляція виділених приміщень.

8.2. Захист мовної інформації: від лазерних систем акустичної розвідки, від несанкціонованого запису, у телефонних лініях.

8.3. Виявлення, ідентифікація та локалізація закладних пристроїв.

9. Захист інформації від витоку по візуально-оптичному каналу

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.

7. Антіпов І.Є., Олейніков А.М., Ликов Ю.В., Кукуш В.Д. , Милютченко І.О. Засоби та системи технічного захисту інформації. Навчальний посібник для студентів ЗВО // Харків: ФОП Панов А.М., 2019. – 216 с.

4. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

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.

8. Скиба В., Курбатов В. Руководство по защите от внутренних угроз информационной безопасности. – Спб: Питер, 2008. – 320 с.

9. 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.

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

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

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

13. 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.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ ВСТУПНИКА ПРИ ПРОВЕДЕННІ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Загальна кількість завдань в тесті – 120. Бланк тестування складається з 30 тестових завдань, які формуються с загальної кількості завдань в тесті. Кількість варіантів бланків – 4.

Тривалість проведення фахового випробування складає 120 хвилин.

Кількість варіантів відповідей у кожному тестовому завданні – 5 (одна відповідь правильна, 4 відповіді не правильні). Вступник має обрати правильну відповідь.

Критерії оцінювання знань вступника відповідно до кількості обраних правильних відповідей з 30 тестових завдань в одному варіанті приведений в таблиці 1.

Таблиця 1 – Критерії оцінювання знань вступника при проведенні фахового вступного випробування

Кількість правильних відповідей	Оцінка фахового випробування	Кількість правильних відповідей	Оцінка фахового випробування	Кількість правильних відповідей	Оцінка фахового випробування
1	не склав	11	105	21	155
2	не склав	12	110	22	160
3	не склав	13	115	23	165
4	не склав	14	120	24	170
5	не склав	15	125	25	175
6	не склав	16	130	26	180
7	не склав	17	136	27	185
8	не склав	18	140	28	190
9	не склав	19	145	29	195
10	100	20	150	30	200