ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____Ігор РУБАН
«__» ____04____ 2023 р.

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

Спеціальність 125 Кібербезпека та захист інформації

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

Протокол засідання приймальної комісії

№ 15 від 18.04. 2023 р.

Голова фахової комісії _____Геннадій ХАЛІМОВ

Відповідальний секретар
приймальної комісії _____Аркадій СНІГУРОВ

Харків 2023

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. І.Д. Горбенко, Т.О. Гріненко. 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. – К.: Видавнича група BHV, 2009. – 608с.

3. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.

4. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А.В. Жилін, О.М. Шаповал, О.А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

5. Кібербезпека мереж наступного покоління: навч. посіб. / О.О. Вараксін, Є.В. Василіу, С.М. Горохов и др.; за ред. В. Г Кононовича ; М-во освіти і науки України, Одеська нац. академія зв'язку ім. О. С. Попова. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 240 с.

6. Конспект лекцій з дисципліни «Безпека безпроводових мереж» для студентів усіх форм навчання спеціальності 125 «Кібербезпека» освітньої програми «Безпека інформаційних і комунікаційних систем» [Електронний ресурс] / упоряд.: О.В. Сєвєрінов, О.І. Федюшин, А.В. Власов. – Електронне

видання. – Харків: ХНУРЕ, 2019. – 118 с. - pdf / 2,32 Mb.

7. Федотова-Півень І.М. Операційні системи: навчальний посібник. [за ред. В.М. Рудницького] / І.М. Федотова-Півень, І.В. Миронець, О.Б. Півень, С.В. Сисоєнко, Т.В. Миронюк; Черкаський державний технологічний університет. – Харків: ТОВ «ДІСА ПЛЮС», 2019. – 216 с.

8. Авраменко В.С., Авраменко А.С. Основи операційних систем. Навчальний посібник. – Черкаси: ЧНУ імені Богдана Хмельницького, 2018. – 524 с.: іл. ISBN 966-552-157-8.

9. 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. Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах: навч. посібник / О.О. Кузнецов, С.Г. Семенов; МОН України, ХНУРЕ. – Харків: ХНУРЕ, 2009. – 184 с.

11. William Stallings Cryptography and Network Security: Principles and Practice, 7th Edition – Pearson Education, 2017. –753 p.

12. Introduction to network security: theory and practice / Jie Wang, Zachary A. Kissel, 2nd Edition. – Wiley, 2015. – 440 p.

13. Pavel Yosifovich, Mark Russinovich, David Solomon, Alex Ionescu. Windows Internals, Part1: System architecture, processes, threads, memory management, and more, 7th Edition – Microsoft Press, 2017. – 800 p. ISBN-10: 9780735684188, ISBN-13: 978-0735684188.

14. Evi Nemeth. UNIX and Linux System Administration Handbook, 5th Edition / Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley, Dan Mackin. – Addison-Wesley Professional, 2017. – 1232 p. ISBN-10: 0134277554, ISBN-13: 978-0134277554.

15. Silberschatz, A., Galvin, P. B., Gagne, G. Operating system concepts. 10th edition. Hoboken, NJ : Wiley, 2018. – 1278 p.

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: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво «Форт», 2013. – 880 с.

3. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво «Форт», 2015. – 960 с.

4. Задірака В., Олексик О. Комп’ютерна криптологія. - Київ, 2002. - 502 с.

5. Кузнецов О.О. Потокові шифри: монографія / О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, Ю.І. Горбенко; за загальною редакцією І.Д. Горбенко. – Харків: Видавництво «Форт», 2019. – 544 с.

6. Сенів М.М. Безпека програм та даних: навч. посіб. / М.М. Сенів, В.С. Яковина; М-во освіти і науки України, Нац. ун-т "Львівська політехніка". – Львів: Вид-во Львівської політехніки, 2015. – 256 с.

7. ISO/IEC 11700-1, 2, 3. Information technology - Security techniques - Key management.

8. ISO/IEC 15946-1, 2, 3. Information technology - Security techniques - Cryptographic techniques based on elliptic curves.

9. ISO/IEC 9798-1, 2, 3, 4, 5. IT Security techniques - Entity authentication.

10. ISO/IEC 9797-1, 2, 3. Information technology - Security techniques - Message Authentication Codes (MACs).

11. ISO/IEC 13888-1.2.3. Information security — Non-repudiation.

12. ISO/IEC 14888- 1.2.3. IT Security techniques — Digital signatures with appendix.

13. ISO/IEC 9594-8. Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks.

14. ISO/IEC 18031. Information technology - Security techniques - Random bit generation.

15. ISO/IEC 18033 – 1, 2, 3, 4. Information technology - Security techniques - Encryption algorithms.

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. – 299 с.

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

3. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. Харків: ХНУРЕ, 2018. – 216 с

4. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник/ Іваненко С.О., Гавриленко О.В., Липский О.А., Швецов А.С. - Киев, ІСЗЗІ НТУУ «КПІ», 2016.- 104 с.

5. Носов В.В., Манжай О.В. Організація та забезпечення безпеки інформації. Навч. посібник: - Харків, Вид-во Харків, Нац. ун-ту внутр. справ, 2007. - 216 с.,

6. Пархуць Л.Т. Методи і засоби захисту інформації. Конспект лекцій. Частина 1. «Захист інформації від витоку по технічних каналах». НУ ЛП, — Львів: 2008. - 67 с.

7. Пархуць Л.Т. Методи і засоби пошуку електронних пристроїв перехоплення інформації Конспект лекцій. Частина 2. . НУ ЛП, — Львів: 2009. — 84 с.

8. 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.

9. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

10. Основи інформаційної безпеки: навч. пос. / Дудикевич В.Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця: ВНТУ, 2018. – 316 с.

11. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

4. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Теми навчальної дисципліни::

1.1. Система міжнародних стандартів ISO27к. Область застосування стандартів. Зміст процесу впровадження створення систем управління інформаційної безпеки (СУІБ). Життєвий цикл СУІБ. 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 СУІБ згідно стандарту ISO/IEC 27001. Політика СУІБ: цілі, зміст, перегляд. Основні етапи впровадження і функціонування СУІБ. 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. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 «Кібербезпека» / О.Г. Корченко, М.С. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванчнко. – Ніжін: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.

2. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

3. В.В. Домарев, Д.В. Домарев. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k), Донецьк: Велстар, 2012. – 146 с.

4. Замула О.А. Нормативно–правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації: навч. посібник. / О.А. Замула, Ю.І. Горбенко, О.І. Шумов. – Харків: ХНУРЕ, 2010. – 248 с.

5. ДСТУ ISO/IEC 27000:2017 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2016, IDT)

6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013, IDT).

8. ДСТУ ISO Guide 73:2013 Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT).

9. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Менеджмент ризиків інформаційної безпеки (ISO/IEC 27005:2011, IDT).

10. ISO/IEC 27035:2011 "Information technology. Security techniques. Information security incident management".

11. NIST SP 800-61 "Computer security incident handling guide".

12. NIST SP 800-39 "Managing Information Security Risk".

13. NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations".

14. NIST SP 800-30 "Guide for Conducting Risk Assessments".

15. NIST SP 800-137 "Information Security Continuous Monitoring"

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 – 3.

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	124	21	164
2	не склав	12	128	22	168
3	не склав	13	132	23	172
4	не склав	14	136	24	176
5	100	15	140	25	180
6	104	16	144	26	184
7	108	17	148	27	188
8	112	18	152	28	192
9	116	19	156	29	196
10	120	20	160	30	200