ПРОГРАМА
фахового вступного випробування
для вступу на навчання для здобуття ступеня вищої освіти магістр
на основі освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека

1. Вступ

Фахове вступне випробування проводиться з метою перевірки знань, умінь та навичок кандидатів на здобуття вищої освіти ступеня магістра. Програма фахового вступного випробування включає перелік навчального матеріалу, який виноситься на фахове випробування та критерії оцінювання курсантів.

Програма вступного фахового випробування на навчання за другим (магістерським) рівнем вищої освіти містить основні теоретичні питання з навчальних дисциплін навчального плану підготовки бакалавра зі спеціальності 125: Кібербезпека:

Прикладна криптологія;

Безпека операційних систем;

Системи технічного захисту інформації;

Комплексні системи захисту інформації: проектування, впровадження, супровід;

Управління інформаційною безпекою.

Фахове вступне випробування проходить у формі письмових тестів з двадцяти теоретичних питань, які входять в одне тестове завдання.

2. Зміст програми

На фахове вступне випробування виноситься матеріал за наступними темами відповідних навчальних дисциплін:

Прикладна криптологія

Схеми симетричної та асиметричної криптосистем, їх переваги та недоліки. Типи атак крипто аналізу та методи їх реалізації. Моноалфавітні та багатоалфавітні шифри підстановки. Методи їх криптоаналізу та аналіз їх стійкості. Шифри перестановки та методи їх криптоаналізу. Сучасні блокові шифри та їх компоненти. Сучасні шифри потоку. Регістри зсуву зі зворотним зв’язком. Стандарти шифрування даних DES, AES, ДСТУ ГОСТ 28147:2009. Схема асиметрично-ключової криптосистеми. Криптографічна система RSA, Рабина, Ель-Гамаля. Дайджест повідомлення. Криптографічна ґеш-функція та її критерії. Процедура перевірки цілісності повідомлення. Код виявлення модифікації повідомлення та код встановлення дійсності повідомлення. Цифровий підпис. Цифровий підпис RSA, Ель-Гамаля. Методи автентифікації об’єктів. Протоколи автентифікації об’єктів з нульовим розголошенням.

Центр розподілу ключів. Метод ключового погодження Діффі-Хелмана. Методи розподілу відкритих ключів. Сертифікат X.509.

Безпека операційних систем

Основні функції підсистеми захисту операційної системи. Загрози безпеки операційної системи. Основні функції підсистеми захисту операційної системи. Методи розмежування доступу в операційних системах. Розмежування доступу до об'єктів операційної системи. Суб'єкти та об'єкти доступу в ОС Windows. Архітектура системи захисту Windows. Характеристика компонентів. Маркер доступу. Структура, опис привілеїв. Дескриптор захисту: визначення, функції, структура. Управління доступом на основі дескриптора захисту. Аудит безпеки Windows. Порядок запису і моніторингу подій безпеки. Архітектура підсистеми автентифікації Windows. ЇЇ функціонування. Проектування захищеної інфраструктури організації на основі Active Directory Domain Service (AD DS). Елементи доступу в операційних системах Windows Server: групи, користувачі, організаційні одиниці. Види груп та їх характеристика. Привілеї різних груп при функціонуванні у домені. Політика аудиту Windows Server 2012 R2. Групові та локальні політики безпеки в ОС Windows Server 2016. Характеристика облікових записів Linux. Конфігураційні файли паролів Linux. Склад та призначення. Групи в ОС Linux. Опис прав доступу в ОС Linux. Аудит в ОС Linux. Автентифікація в ОС Linux. Модулі автентифікації PAM. Брандмауер Linux iptables. Застосування та налаштування правил. Характеристика облікових записів Linux. Групи в ОС Linux. Брандмауер Linux iptables. Застосування та налаштування правил Linux iptables. Опис прав доступу в ОС Linux.

Системи технічного захисту інформації

Інформація як об'єкт захисту. Властивості та критерії захищеності інформації. Модель технічного каналу витоку інформації. Об'єкт інформаційної діяльності: характеристика елементів, схема. Акустичні канали витоку інформації. Класифікація, методи та засоби захисту. Генератори та види шумових завад. Характеристика, структурні схеми. Системи віброакустичного захисту. Склад, призначення, встановлення. Електромагнітні канали витоку інформації. Класифікація, методи та засоби захисту. Радіозакладні пристрої: класифікація, маскування, схеми та принцип дії. Засоби пошуку радіозакладних пристроїв на ОІД. Методика пошуку радіо закладних пристроїв. Нелінійні локатори. Принципи виявлення, призначення, структурна схема побудови, методика пошуку закладних пристроїв. Електричні КВІ. Класифікація, методи та засоби захисту. Методи та засоби захисту від витоку електричними КВІ. Методи та засоби захисту телефонних ліній.

Комплексні системи захисту інформації: проектування, впровадження, супровід

Порядок проведення робіт зі створення КСЗІ. Етапи створення КСЗІ. Структура комплексної системи захисту інформації. Розроблення технічного завдання на створення КСЗІ в ІТС. Розроблення проекту КСЗІ. Введення комплексної системи захисту інформації в дію та оцінювання захищеності

інформації в ІТС. Організація та проведення експертизи КСЗІ. Порядок створення комплексу ТЗІ. Організація та проведення атестації КТЗІ. Функції служби захисту інформації під час створення і супроводження КСЗІ. Модель загроз об’єкту інформаційної діяльності. Вимоги до захисту інформації в ІТС від несанкціонованого доступу.

Управління інформаційною безпекою

Формування політики інформаційної безпеки в організації. Завдання й функції служби ІБ. Принципи організації служби захисту інформації. Документи служби (положення, інструкції). Основні поняття управління ризиками ІБ. Основні етапи управління ризиками ІБ. Управління ризиками. Модель безпеки з повним перекриттям. ISO / IEC 15408. Критерії оцінки безпеки інформаційних технологій. Стандарт ISO/IEC 27001. Модель багаторівневого захисту.

3. Критерії оцінювання фахового вступного випробування

Під час проведення фахового вступного випробування курсантам забороняється користуватися будь-яким допоміжним матеріалом.

Фахове вступне випробування проводиться лише за затвердженим головою приймальної комісії комплектом тестових завдань.

Для написання фахового вступного випробування курсантам надається не більше однієї академічної години.

Оцінювання знань вступників здійснюється за системою ECTS (100-бальною шкалою).

Сума балів	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	Відмінно
80-89	B	Добре
65-79	C	
55-64	D	Задовільно
50-54	E	
35-49	Fx	Незадовільно
1-34	F	

Фахове вступне випробування проходить у вигляді письмових тестів. Тестове завдання складається з двадцяти теоретичних питань, кожне з яких має по чотири варіанти відповіді, позначені літерами (А, Б, В, Г), серед яких лише один варіант правильний. Для відповідей на питання тестового завдання вступнику надається особистий бланк відповідей. Обираючи правильний, на його думку, варіант відповіді, вступник робить позначку в особистому бланку відповідей шляхом обведення букви, яка відповідає правильній відповіді.

Якщо вступник вирішив виправити відповідь на питання тестового завдання, то має в особистому бланку відповідей позначити іншу відповідь, перекреслити попередню та поставити особистий підпис біля здійсненого виправлення.

Кожна правильна відповідь на питання оцінюється в 5 (п’ять) балів, неправильна відповідь – 0 (нуль) балів.

Вважається, що вступник склав фахове вступне випробування, якщо він отримав не менше 50 балів.

Особисті бланки відповідей, на яких не вказаний шифр або варіант завдання, зроблені помітки невстановленого зразку, або відсутні підписи біля виправлених варіантів відповідей, до розгляду не приймаються.

4. Список літератури

З дисципліни Прикладна криптологія:

1. *Алферов А.П., и др.* Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001. – 480 с.

2. *Фороузан А.Б.* Криптография и безопасность сетей: Учебное пособие. – М.: 2010. – 784 с.

3. *Ємець В., Мельник А., Попович Р.* Сучасна криптографія. Основні поняття. – Львів: Бак, 2003. – 144 с.

4. *Поповский В.В.* Основы криптографической защиты информации в телекоммуникационных системах. Ч. 1./В.В. Поповский, А.В. Персиков. – Х.: «Компания СМИТ», 2010. – 352 с.

5. *Поповский В.В.* Основы криптографической защиты информации в телекоммуникационных системах. Ч. 2./В.В. Поповский, А.В. Персиков. – Х.: «Компания СМИТ», 2010. – 564 с.

6. *Столингс В.* Криптография и защита сетей. Принципы и практика. – Москва. Санкт-Петербург. Киев, 2001. – 668.

7. *Шнайер Б.* Прикладная криптография 2-е издание Протоколы, алгоритмы и исходные тексты на языке С. – Издательский дом «Вильямс», 2005, – 424с.

8. *Венба М.* Современная криптография. Теория и практика. – Учебное пособие. – С.П.-М., 2005. – 760 с.

9. *Харин Ю.С.* Математические основы криптологии: Учебное пособие. – Мн.: БГУ, 1999. – 319 с.

10. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

11. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.: ил.

12. *Коркішко Т., Мельник А., Мельник В.* Алгоритми та процесори блокового шифрування. – Львів: Бак, 2003. – 168 с.

13. *Чмора А.Л.* Современная прикладная криптография. – М.: Гелиус АРВ, 2001. - 244 с.

14. *Фомичев В.М.* Методы дискретной математики в криптологии: Курс лекций. – М.: ДИАЛОГ-МИФИ, 2010 – 422 с.

15. Національний стандарт України ДСТУ 7624:2014. Алгоритм симетричного блокового перетворення.

16. Національний стандарт України ДСТУ 7624:2014. Функція хешування.

17. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: видавництво «Форт», 2012. – 880 с.

З дисципліни Безпека операційних систем:

1. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.

2. *Грайворонский М.В., Новіков О.М.* Безпека інформаційно- комунікаційних систем. - Київ. видавнича група BHV, 2009.- 607 с.

3. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. – ДМК Пресс, 2002. – 656 с.

4. *Моримото Р.* Windows Server 2008 R2. Полное руководство. / Р. Моримото, М. Ноэл, О. Драуби, Р. Мистри, К. Амарис. – М.: Виьямс, 2012.– 1456 с.

5. *Немет Э.* Руководство администратора Linux. Второе издание / Э. Немет, Г. Снайдер, Т. Хейн.–М.: Издательский дом «Вильямс», 2011.–1072 с.

6. *Антонюк А.А.* Захист інформації в автоматизованих системах.

7. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях. М: "Радио и связь", 2001. – 376 с.

8. *Соколов А.В., Шаньгин В.*Ф. Защита информации в распределенных корпоративных сетях и системах. – ДМК Пресс, 2002. – 656 с.

9. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 672 с.

10. *Олифер В.Г., Олифер Н.А.* Новые технологии и оборудование IP-сетей. – СПб.: БХВ- Петербург, 2000. – 512 с.

11. *Ричард Э. Смит*. Автентификация: от паролей до открытых ключей. – Москва. Санкт-Петербург. Киев. 2002.

12. *Проскурин В.Г., Крутов С.В.,* Мацкевич И.В. Защита в операционных системах. – Москва, 2000. – 165 с.

З дисципліни Системи технічного захисту інформації:

1. *Шевченко А. С., Самойлов І. В., Мазулевський О.Є., Артюх С. Г* Навчальний посібник: Комплексні системи захисту інформації інформаційно-телекомунікаційних систем. Частина 1. Основи організації та забезпечення технічного захисту інформації – К.: ВІТІ, кафедра № 33, 2017. – 125 с.

2. *Мазулевський О. Є., Самойлов І. В., Шевченко А. С.* Навчальний посібник: Захист інформації в телекомунікаційних системах і мережах Частина І / – К.: ВІТІ, 2015. – 258 с.

3. *Ленков С.В., Перегудов Д.А., Хорошко В.А.* Методы и средства защиты информации. К.: Арий, 2008. Том І. Несанкционированное получение інформації.- 464 с.

4. *Ленков С.В., Перегудов Д.А., Хорошко В.А*. Методы и средства защиты информации. К.: Арий, 2008. Том II. Інформационная безопастность.- 344 с.

5. Технічні канали витоку інформації. Навчальний посібник / *Ю.Б. Науменко, Н.А. Паламарчук, С.А. Паламарчук, О.Є. Ткаленко*. – К.: ВІТІ НТУУ «КПІ», 2010. – 393 с.

6. *Богданов В.В.* Методи та засоби інженерно-технічного захисту інформації. Частина 1. Навчальний посібник / В.В. Богданов, О.В. Волков, О.В. Жук, В.В. Мартинюк. – К.: ВІТІ ДУТ, 2015. – 244 с.

7. *Грайворонский М.В., Новіков О.М.* Безпека інформаційно- комунікаційних систем. – Київ. видавнича група BHV, 2009. – 607 с.

8. *Зайцев А.П., Шелупанов А.А. , Мещеряков Р.В., Скрыль С.В., Голубятников И.В.* Технические средства и методы защиты информации. М.: Машиностроение, 2009. – 508с.

3 дисципліни Комплексні системи захисту інформації: проектування, впровадження, супровід:

1. *Шевченко А. С., Самойлов І. В., Мазулевський О.Є., Артюх С. Г* Навчальний посібник: Комплексні системи захисту інформації інформаційно-телекомунікаційних систем. Частина 1. Основи організації та забезпечення технічного захисту інформації – К.: ВІТІ, кафедра № 33, 2017. – 125 с.

2. *Мазулевський О. Є., Самойлов І. В., Шевченко А. С.* Навчальний посібник: Захист інформації в телекомунікаційних системах і мережах Частина І / – К.: ВІТІ, 2015. – 258 с.

3. Комплексні системи захисту інформації інформаційно-телекомунікаційних систем. Збірник нормативних документів. – К.: ВІТІ, кафедра № 12, 2016. – 484 с.

4. *Грайворонский М.В., Новіков О.М.* Безпека інформаційно- комунікаційних систем. - Київ. видавнича група BHV, 2009.- 607 с.

5. *Ленков С.В., Перегудов Д.А., Хорошко В.А.* Методы и средства защиты информации. Несанкционированное получение информации. В 2 т. Т. 1. -339 с.

6. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

7. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

8. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

9. НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

3 дисципліни Управління інформаційною безпекою:

1. Системи менеджменту інформаційної безпеки: навч. посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк. – Львів: Видавництво Львівскої політехніки, 2012. – 232 с.

2. *Данилин А.*, *Слюсаренко* А. Архитектура и стратегия. "Инь" и "янь" информационных технологий. - Интернет-университет информационных технологий - ИНТУИТ.ру, 2005

3. *Черкашин П.* Стратегия управления взаимоотношениями с клиентами (CRM). - БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру, 2007

4. *Цирлов В.Л.* Основы информационной безопасности автоматизированных систем. Краткий курс. – М.: Феникс, 2008 – 173с.

5. *Петренко В.А.* Управление информационными рисками: Информационно-методическое пособие по курсу повышения квалификации „Анализ рисков в области защиты информации” - Санкт-Петербург: «Издательский Дом «Афина», 2009 год – 387.

6. ISO 27002:2005 “Руководство по управлению информационной безопасностью”.

7. ISO 27005:2008 “Управление рисками информационной безопасности”.

8. ISO 27001:2005 “Требования к системе управления информационной безопасностью”.