МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ЛОПАТОВСЬКИЙ
«__» _____ 2023 р.

ПРОГРАМА ФАХОВОГО ІСПИТУ

для вступу на навчання для здобуття ступеня вищої освіти «магістр» на основі раніше здобутого ступеня вищої освіти бакалавра, магістра (освітньо-кваліфікаційного рівня спеціаліста)

Галузь знань: 12 – «Інформаційні технології»
Спеціальність: 125 – «Кібербезпека та захист інформації»
Освітня програма: «Кібербезпека та захист інформації»

Схвалено на засіданні кафедри кібербезпеки
протокол № 12 від 10 квітня 2023 р.

Зав. кафедри _____ Юрій КЛЬОЦ

Гарант ОП _____ Віра ТІТОВА

Програма розглянута та схвалена на засіданні
вченої ради факультету інформаційних технологій
протокол № 4 від 14 квітня 2023 р.

Голова вченої ради ФІТ _____ Олег САВЕНКО

Хмельницький – 2023

Загальні положення

Вступний фаховий іспит проводиться приймальною комісією Хмельницького національного університету за спеціальністю 125 – «Кібербезпека та захист інформації», ОПП «Кібербезпека та захист інформації» для вступників на навчання для здобуття ступеня вищої освіти «магістр» на основі раніше здобутого ступеня вищої освіти бакалавра, магістра (освітньо-кваліфікаційного рівня спеціаліста).

Мета вступного фахового іспиту полягає у перевірці здатності абітурієнта до опанування освітньої програми «Кіберебезпека та захист інформації» другого (магістерського) рівня вищої освіти на основі здобутих раніше компетентностей з таких освітніх компонентів, як: комплексні системи захисту інформації, захист інформації в інформаційно-комунікаційних системах, теорія передачі і захисту даних (теорія інформації та кодування), прикладна криптологія.

Технологія проведення вступного фахового іспиту

Вступний іспит (вступне випробування) проводиться у формі тестування із комп'ютерною обробкою результатів. Система проведення вступних іспитів є оригінальною розробкою ХНУ і захищена свідоцтвом про авторське право № 39534 від 08.08.2011 р. Вона розроблена на підставі таких документів: Закону України «Про вищу освіту», «Положення про приймальну комісію ХНУ», Порядку прийому до вищих навчальних закладів України та Правил прийому до Хмельницького національного університету.

Основні положення системи тестування із комп'ютерною обробкою результатів викладені нижче. Бази даних тестових завдань створюються для всіх дисциплін, з яких проводиться тестування, щорічно поповнюються і вдосконалюються.

Бази даних тестових завдань або навчальні програми, за якими вони створені, є відкритими. Університет щорічно оприлюднює їх у паперовому або в електронному вигляді.

Відповідальність за зміст і якість тестових завдань покладається на голову предметної комісії.

Екзаменаційний білет може містити тестові завдання одного або різних рівнів складності. Для автоматизованого формування білетів використовують комплекс комп'ютерних програм, які компонують бази даних тестових завдань з кожної дисципліни, формують екзаменаційні білети за допомогою випадкової вибірки та роздруковують їх.

Екзаменаційні білети, що включають тестові завдання, формують і тиражують комп'ютерними засобами перед початком тестування. Сформовані білети засвідчуються печаткою приймальної комісії.

Номер кожного екзаменаційного білета збігається з номером талона відповідей, який додається до нього.

Організація автоматизованого формування комплекту екзаменаційних білетів до вступних іспитів, контроль за ним покладається на відповідального секретаря Приймальної комісії або його заступника.

Тестування проводиться відповідно до розкладу в аудиторіях, що обладнані необхідними технічними засобами.

Пропуск вступників до аудиторії тестування проводить відповідальний секретар ПК та його заступники. При цьому перевіряється паспорт та перепустка, у якій вказана особа вступника, дата і час тестування.

Кожний учасник тестування витягує номер, який вказує його місце в аудиторії. Всі місця за столами пронумеровані.

В аудиторії тестування дозволяється присутність громадських спостерігачів (батьків вступників).

Вступникам видаються титульні листи і проводиться роз’яснення щодо їх заповнення.

Після розміщення учасників тестування в аудиторії вступники особисто вибирають екзаменаційні білети, що розкладені на столі.

Після отримання екзаменаційних білетів вступники працюють над розв’язком завдань протягом встановленого часу.

Талони відповідей надаються кожному вступнику в одному екземплярі. Забороняється видача вступнику другого талона. Талон відповідей заповнюється вступником відповідно до роз’яснення щодо їх заповнення.

Після закінчення роботи над тестами, або добігання до кінця часу, відведеного на тестування, вступники здають підписані роботи разом з талонами відповідей, які до початку сканування знаходяться на столі екзаменатора.

Сканування талонів відповідей починається після здачі робіт всіма вступниками у їх присутності. Процес сканування талонів відповідей демонструється за допомогою проектору на великому екрані.

Після закінчення сканування та комп'ютерної обробки талонів відповідей результати тестування демонструються на екрані у вигляді екзаменаційної відомості, в якій відсутні прізвища вступників, а є лише номер екзаменаційного білета. Далі персонал приймальної комісії вносить в комп’ютер інформацію про відповідність номера екзаменаційного білета прізвищу вступника. На екрані демонструється екзаменаційна відомість з прізвищами вступників, яка роздруковується і завіряється відповідальним секретарем приймальної комісії.

Критерії оцінювання вступних іспитів затверджуються на засіданні Приймальної комісії та наводяться в додатку до Правил прийому.

Перелік освітніх компонентів (навчальних дисциплін), на базі яких складається іспит

1. Комплексні системи захисту інформації

Перелік тем, на базі яких складаються тестові завдання

Принципи організації КСЗІ. Концептуальні підходи до проєктування систем захисту. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі (ІТС). Етапи створення КСЗІ в ІТС. Формування технічного завдання на створення КСЗІ в ІТС. Базові розділи ТЗ. Нормативний супровід розробки ТЗ. Розробка ескізного проєкту КСЗІ. Представлення схем, структур, елементів КСЗІ. Оформлення та представлення текстової документації. Розробка комплекту документації для етапу проєктування КСЗІ. КСЗІ в критичній інфраструктурі.

Класифікація загроз інформаційній безпеці, ознаки класифікації. Ознаки моделі порушника, як етапу побудови КСЗІ. Категорії порушників. Класифікація порушника. Поняття контрольована зона. Модель загроз для ідентифікації каналів витоку інформації. Джерело загрози. Перелік загроз з визначенням порушень властивостей інформації та ІТС.

Джерела та носії інформації. Типова структура та види технічних каналів витоку інформації. Електричні канали витоку інформації. Електромагнітні канали витоку інформації. Радіоканали втрат інформації. Методи та засоби захисту від витоку інформації.

Список рекомендованої літератури

1. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник/ Г. І. Ластівка, П. М. Шпатар. Чернівці: Чернівецький національний університет, 2018. 252 с.
2. Комплексні системи захисту інформації: навчальний посібник/ Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін. Вінниця: ВНТУ, 2018. 118 с.
3. 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.
4. Методи та засоби технічного захисту інформації. Опорний конспект лекцій: навч. посіб./ КПІ ім. Ігоря Сікорського; уклад.: В. М. Луценко, Д. О. Прогонов. Київ: КПІ ім. Ігоря Сікорського, 2021. 289 с.
5. Інформаційна безпека: навчальний посібник/ [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.

2. Захист інформації в інформаційно-комунікаційних системах

Перелік тем, на базі яких складаються тестові завдання

Ідентифікація користувачів. Аутентифікація користувачів. Протоколи ідентифікації та аутентифікації. Технічні засоби ідентифікації і аутентифікації. Носії ключової інформації (флеш пам’ять, електронні ключі, SMART-карти, пристрої Touch-Memory). Електронні ключі. Сертифіковані ключі, стандарт X.509. Сфери застосування інфраструктури відкритих ключів та цифрових сертифікатів.

Типи шкідливого ПЗ. Класифікація шкідливих програм. Основи роботи антивірусних програм. Сигнатурний аналіз. Евристичні аналізатори. Поведінкові блокатори. Протидія шкідливому коду. Шкідливе ПЗ для мобільних пристроїв. Етапи забезпечення антивірусного захисту. Концепція антивірусної безпеки. Політика антивірусної безпеки. Антивірусні комплекси. Структура та алгоритми роботи антивірусних комплексів.

Завдання безпеки комп’ютерних та бездротових мереж. Фізичний захист мереж. Програмні та апаратні засоби захисту мереж. Адміністративні заходи безпеки комп’ютерних мереж. Поняття мереж. Типи мереж. Апаратні та програмні компоненти мереж. Мережні топології. Модель OSI. Модель TCP.

Мережні протоколи. Протоколи дротових і бездротових мереж. Стандартні порти. Мережні служби. Клієнт-серверна архітектура. DHCP-сервер. DNS сервер. Сервер друку. Файловий сервер. Веб сервер. Поштовий сервер. Проксі сервер. Сервер автентифікації. Syslog сервер.

Основні мережні пристрої. Мережна інтерфейсна карта. Повторювачі, мости та концентратори. Керовані та некеровані комутатори. Бездротові точки доступу. Маршрутизатори. Міжмережні екрани. Пристрої UTM. Мережна адресація. MAC адреси. IP адреси.

Список рекомендованої літератури

1. Інформаційна безпека: навчальний посібник/ [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
2. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навч. посіб./ В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. Хмельницький: ХНУ, 2021. 174 с.
3. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.

4. Організація комп’ютерних мереж: підручник/ Ю.А. Тарнавський, І.М. Кузьменко. Київ: КПІ ім. І. Сікорського, 2018. 259 с.
5. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: Мографія. В.Л. Бурячок, В.Ю. Соколов. Київ: КУБГ, 2019. 164 с.
6. Безпека безпроводових і мобільних мереж: Навчальний посібник/ В. Ю. Соколов, В. Л. Бурячок, М. М. Тадждіні / ред. перекл. О. П. Райтер. 2 вид., доп. – К.: КУБГ, 2019. 130 с.
7. Інформаційна безпека в комп’ютерних мережах: навч. посіб./[О.А. Смірнов, О.К. Конопліцька-Слободенюк, С.А. Смірнов, К.О. Буравченко та ін.]. Кропивницький: Видавець Лисенко В.Ф., 2020. 295 с.

3. Теорія передачі і захисту даних / Теорія інформації та кодування

Перелік тем, на базі яких складаються тестові завдання

Інформація, дані і сигнали як об’єкт захисту. Кількісна оцінка інформації. Ентропія. Дискретні і безперервні повідомлення і сигнали. Цифрова обробка сигналів. Ентропія безперервних розподілів, передача безперервних повідомлень.

Ефективне (оптимальне) кодування. Завадостійке (надлишкове) кодування. Блокові завадостійкі корегуючі коди. Циклічні коди.

Поняття, основні характеристики і синтез комбінаційних схем цифрових вузлів. Перетворювачі кодів. Застосування перетворювачів кодів для реалізації криптографічних шифрів заміни. Шифратори і дешифратори та їх застосування в електронних системах захисту.

Список рекомендованої літератури

1. Теорія інформації та кодування в прикладах і задачах : навч. посібник/ А. В. Івашко, В. А. Крилова ; Нац. техн. ун-т "Харків. політехн. ін-т". Харків : НТУ "ХПІ", 2022. 317 с.
2. Теорія інформації та обробка сигналів: конспект лекцій: навч. посіб./ Ю. С. Ямненко, К. С. Клен. Киів: КПІ іМ. Ігоря Сікорського, 2019. l20 с.
3. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія/ Ю. М. Бойко, В. А. Дружинін, С. В. Толюпа. Київ: Логос, 2018. 227 с.
4. Кодування джерел інформації та каналів зв'язку: навчальний посібник/ Л.Н. Беркман, А.П. Бондарчук, Г.І. Гайдур, Н.С. Чумак. Київ: ННІТІ ДУТ, 2018. 9l с.

4. Прикладна криптологія

Перелік тем, на базі яких складаються тестові завдання

Поняття криптографічної системи. Безумовно-стійкі криптографічні системи і їх реалізація. Поняття та умови реалізації обчислювально-стійких криптосистем. Класифікація і характеристика доказово-стійких криптосистем.

Афіні шифри. Потокові шифри. Блокові і складені шифри. Симетричні та асиметричні шифри. Спрямоване шифрування. Методи забезпечення цілісності та достовірності у класі симетричних шифрів.

Криптосистеми з відкритими ключами і відкритим розподілом ключів. Розподіл ключів по схемі Діффі-Гелмана. Поняття та властивості цифрового підпису. Підписи в класі перетворень Ель-Гамаля та RSA. Поняття хеш-функції. Криптоперетворення в групах точок еліптичних кривих (ЕК).

Алгоритми і засоби формування ключів і паролів. Оцінка стійкості і складності ключів. Поняття, задачі та інструменти криптоаналізу. Атаки на ключі та паролі.

Список рекомендованої літератури

1. Криптологія: навч. посібник/ М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. К.: Видавничий дім «Кондор», 2020. 248 с.
2. Криптологія: опорний коспект лекцій/ уклад.: Д. Вербівський, Б. Якимчук. Житомир: Вид-во ЖДУ ім. Івана Франка, 2023. 173 с.
3. Криптоаналіз. Криптографічні протоколи: навчальний посібник/ О. М. Гапак. ДВНЗ «УжНУ», 2021. 93 с.
4. Криптографія від історії до сучасних стандартів: навч. посібник/ Г. Л. Козіна. Запоріжжя : НУ «Запорізька політехніка», 2020. 192 с.
5. Інформаційна безпека: навчальний посібник/ [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
6. Технології захисту інформації/ Ю. А. Тарнавський. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.