ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____ В.В.Семенець
«27» 02 2018 р.

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
для вступу на освітній ступень магістра

Спеціальність: 125 Кібербезпека
Спеціалізація: “Безпека інформаційних і комунікаційних систем”
“Безпека державних інформаційних ресурсів”

Протокол засідання приймальної комісії
№ 28 від 27.02. 2018 р.

Голова фахової
атестаційної комісії _____ Г.З.Халімов

Відповідальний секретар
приймальної комісії _____ А.В.Снігуров

Харків-2018

1.Дисципліна «Прикладна криптологія»

автор тесту та специфікації проф. каф. БІТ Халімов Г.З.

Перелік тем (за робочою програмою):

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.

2.Дисципліна «Інформаційні технології»

автор тесту та специфікації проф. каф. БІТ Семенов С.Г.

Перелік тем (за робочою програмою):

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 фізичною та канального рівнів. Характеристики ліній передачі даних на основі різних середовищ. Методи множинного доступу до каналу передачі даних. 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. Принципи, технологи, протоколы: Учебник для вузов - СПб.: Питер, 2006 - 958 с.

3.Дисципліна «Захист інформації в інформаційно-комп'ютерних системах»

автор тесту та специфікації доц. каф. БІТ Федюшин О. І.

Перелік тем (за робочою програмою):

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.

2.3. ASN/ 1.

2.4. Протокол LDAP. Інформаційна модель.

2.5. Протокол LDAP. Функціональна модель.

2.6. 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)

Навчальна література:

1. Вильям Столлингс. Основы защиты сетей. Приложения и стандарты. М.:Вильямс, 2002. - 432 с.

2. Ричард 3. Смит. Аутентификация: от паролей до открытых ключей. — М.: Вильямс, 2002. — 415 с.

4.Дисципліна "Нормативно правове забезпечення інформаційної безпеки"

автор тесту та специфікації проф. каф. БІТ Замула О.А.

Перелік тем (за робочою програмою):

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.

1.4. 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 - 7 с.

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

5.Дисципліна «Системи технічного захисту інформації»
автор тексту та специфікації проф. кафедри БІТ Заболотний В.І.

Перелік тем (за робочою програмою):

1. Технічні канали витоку інформації. Види, джерела та носії інформації, що підлягає захисту. Структура технічних каналів витоку інформації. Аналіз та класифікація ТКВІ.

1.1. Небезпечні сигнали та їх джерела. Дискретні сигнали та їх спектри в основних технічних засобах (ОТЗ). Аналогові сигнали, їх спектри та спотворювання в ОТЗ.

1.2. Побічні електромагнітні випромінювання та наведення. Елементи електричних схем ОТЗ як випромінювачі побічних електромагнітних полів.

1.3. Прийом побічних електромагнітних випромінювань та наведень. Вузькосмугові засоби прийому. Широкосмугові засоби прийому. Наведення електромагнітних полів на випадкові антени.

2. Концепція і методи технічного захисту інформації. Елементи ТЗІ на ОІД. Класифікація заходів та засобів ТЗІ. Показники та норми ТЗІ. Пасивні засоби ТЗІ. Активні засоби ТЗІ. Організаційні заходи ТЗІ.

2.1. Екранування інформативних полів. Фізичні основи екранування і компенсації електромагнітних полів. Показники екранування. Конструкції екранів та екранованих споруд.

2.2. Подавлення. інформативних сигналів в колах заземлення та електроживлення. Фільтри живлення: характеристики, призначення, конструкція, застосування. Заземлення на ОІД, його призначення. Характеристики системи заземлення.

2.3. Активний захист інформації. Активні перешкоди та їх характеристики. Засоби створення активних перешкод. Заглушування інформативних сигналів в просторі, комунікаціях, системах заземлення та електроживлення.

2.4. Зовнішній вплив на інформацію, що циркулює у технічних засобах. Шляхи створення сигналів впливу на ТЗШ. Захист технічних засобів від деструктивного впливу електричними та електромагнітними полями.

2.5. Захист мовної інформації. Спрямовані мікрофони та їх можливості. Енергетичне приховування акустичних інформативних сигналів. Звукоізоляція та звукопоглинання виділених приміщень. Способи та засоби боротьби із закладними пристроями.

2.6. Захист від видової розвідки. Видова розвідка, її основні характеристики та можливості. Приховування об'єктів спостереження.

2.7. Організація ТЗІ в Україні. Державна система технічного захисту інформації. Державні органи системи ТЗІ.

2.8. Контроль ТЗІ. Способи контролю. Контроль ефективності технічного захисту інформації. Методи розрахунку та інструментального контролю показників захисту інформації. Апаратура контролю.

2.9. Технічна охорона об'єктів інформаційної діяльності. Методи і засоби технічної охорони об'єктів. Задачі і способи охорони об'єктів. Принципи побудови системи охорони. Засоби охорони та їх характеристики. Засоби відеоспостереження.

Навчальна література:

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Изд-во ЮНИОР; 2003.-504 с., ил.

2. Електронний ресурс http://simetronn.net78.net/?&sitemap.

3. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

4. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ - ПЕМВН- 95).

Затверджено на засіданні кафедри БІТ протокол № 7 від "17" січня 2018 року.

Зав. каф. БІТ _____ Халімов Г.З.