МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ЗАТВЕРДЖУЮ
Ректор Державного університету
телекомунікацій

В.Б. Толубко

«___» _____ 2016 р.

ПРОГРАМА
ВСТУПНИХ ВИПРОБУВАНЬ

кандидатів на навчання в аспірантурі
за спеціальністю «125 - кібербезпека»

Київ – 2016

Абітурієнт з освітнім ступенем (освітньо-кваліфікаційним рівнем) **магістр (спеціаліст)** повинен **знати:**

- основні напрями розвитку системи управління інформаційною безпекою;
- загальну методологію та структуру організаційного забезпечення інформаційної безпеки на рівні підприємства (організації);
- основи управління інформаційною безпекою на рівні підприємства (організації);
- нормативно-правову базу з питань управління інформаційною безпекою;
- організацію надання послуг у сфері інформаційної безпеки.

вміти:

- аналізувати загрози інформаційній безпеці;
- застосовувати системний підхід для побудови системи управління інформаційною безпекою підприємства (організації);
- планувати діяльність служби безпеки підприємства (організації);
- проектувати та реалізовувати комплексну систему захисту інформації підприємства (організації) до вимог нормативних документів;
- проводити перевірку установ, організацій та підприємств щодо виконання вимог правових норм і стандартів стосовно ліцензування й сертифікації в області інформаційної безпеки;
- здійснювати оцінку відповідності системи управління інформаційною безпекою своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.

ПРОГРАМИ ФАХОВОГО ВИПРОБУВАННЯ

РОЗДІЛ 1.

Тема1.1. Основні поняття управління інформаційною безпекою

Поняття інформаційної безпеки. Проблеми інформаційної безпеки та управління нею.

Тема 1.2. Методи управління інформаційною безпекою

Класифікація методів управління. Метод наукового управління. Метод адміністративного управління. Метод людських відносин. Метод кількісного підходу в управлінні.

Тема 1.3. Основні підходи до управління інформаційною безпекою

Процесний підхід в управлінні. Переваги та недоліки процесного підходу. Використання процесного підходу в управлінні інформаційною безпекою. Системний підхід в управлінні. Переваги та недоліки системного підходу. Використання системного підходу в управлінні інформаційною безпекою. Ситуаційний підхід в управлінні. Переваги та недоліки ситуаційного підходу. Використання ситуаційного підходу в управлінні інформаційною безпекою. Використання комбінацій різних підходів в управлінні інформаційною безпекою.

Тема 1.4. Політика інформаційної безпеки

Поняття політики інформаційної безпеки. Цілі та задачі політики інформаційної безпеки. Верхній, середній та нижній рівні політики безпеки. Розробка політики інформаційної безпеки на різних рівнях управління.

Тема 1.5. Програма управління інформаційною безпекою

Програми верхнього та нижнього рівнів. Розробка програми управління інформаційною безпекою. Синхронізація програми безпеки з життєвим циклом інформаційної системи. Коригування програми управління інформаційною безпекою в залежності від зміни політики інформаційної безпеки чи складу інформаційної системи.

Тема 1.6. Основні класи заходів процедурного рівня

Заходи процедурного рівня в процесі управління інформаційною безпекою. Управління персоналом. Фізичний захист. Підтримка працездатності інформаційної системи. Реагування на порушення режиму безпеки. Планування

відновлюваних робіт. Особливості управління персоналом у сфері інформаційної безпеки.

Тема 1.7. Адміністративні заходи забезпечення інформаційної безпеки

Ранжування користувачів інформаційних ресурсів. Сертифікація та навчання користувачів. Основні заходи забезпечення інформаційної безпеки щодо персоналу. Управління ризиками. Координація діяльності в області інформаційної безпеки. Поповнення і розподіл ресурсів. Стратегічне планування. Контроль діяльності в області інформаційної безпеки.

Тема 1.8. Правові аспекти управління інформаційною безпекою

Рівні інформаційної безпеки. Місце законодавчого рівня забезпечення інформаційної безпеки у питаннях захисту інформації. Класифікація інформації. Схема класифікації інформації. Інформація з обмеженим доступом. Законодавчі акти та інші нормативні документи з питань інформаційної безпеки. Основні стандарти інформаційної безпеки. Хто визначає належність інформації до певної категорії. Роль мережі Інтернет в інформаційному забезпеченні законотворчого процесу. Проблеми інформаційної безпеки в процесах глобалізації економіки. Гармонізація законодавчої бази держав у сфері інформаційної безпеки.

Тема 1.9. Проблеми безпеки інформаційної інфраструктури

Поняття інформаційної інфраструктури. Об’єкти забезпечення інформаційної безпеки. Джерела загроз інформаційній безпеці. Основні заходи захисту інформаційної інфраструктури. Заходи захисту території та приміщень. Заходи захисту від технічних засобів шпигунства. Заходи захисту АІС. Особливості управління персоналом у сфері інформаційної безпеки. Управління інформаційною безпекою бізнесу.

Тема 1.10. Управління захистом автоматизованих робочих місць

Поняття автоматизованого робочого місця (АРМ). Технічне, програмне, інформаційне та організаційне забезпечення АРМ. Дослідження загроз інформаційній безпеці АРМ і необхідність його захисту. Інформаційні процеси АРМ та їх структура. Автоматизована система документообігу АРМ. Контроль рівня захисту конфіденційних документів АРМ. Управління захистом інформації АРМ.

Тема 1.11. Управління інформаційною безпекою в умовах кризи

Прояви кризи в економіці. Заходи служби інформаційної безпеки в умовах кризи: оптимізація асортиментна продукції, зміна стратегії продажів, скорочення витрат на персонал, підвищення продуктивності, аутсорсинг, офшоринг,

оптимізація використання та вартості залучення ресурсів. Дії керівників служби інформаційної безпеки: скорочення персоналу та альтернативні заходи, захист бізнесу від додаткових витрат, пов'язаних із діями звільнених співробітників, тоталітаризм керівника служби інформаційної безпеки в умовах кризи, розробка стратегії виживання служби інформаційної безпеки в умовах кризи.

Тема 1.12. Управління інформаційною безпекою у надзвичайних ситуаціях

Поняття надзвичайного стану. Загальні характерні особливості всіх видів стихійного лиха. Причини запізнення реакції на надзвичайну ситуацію. Рівні поінформованості про надзвичайну ситуацію. Інформаційні фільтри для даних про надзвичайну ситуацію. Інформаційна система в системі управління надзвичайною ситуацією. Основні цілі використання інформаційної системи в умовах надзвичайних ситуацій. Планування дій в умовах надзвичайної ситуації. Планування безперебійної роботи інформаційної системи в умовах надзвичайної ситуації. Створення контрольного списку заходів на випадок надзвичайної ситуації.

Тема 1.13. Аналіз ризиків в управлінні інформаційною безпекою

Управління ризиками як одна з головних цілей програми безпеки організації. Процес управління ризиками: вибір об'єктів для аналізу, вибір методології оцінки ризиків, ідентифікація активів, аналіз загроз та їх наслідків, оцінка ризиків по кожному об'єкту, вибір захисних заходів, реалізація та перевірка обраних заходів, оцінка залишкового ризику.

Тема 1.14. Економіка інформаційної безпеки

Основні проблеми економіки інформаційної безпеки. Визначення економічної безпеки для підприємства. Зв'язок економічної та інформаційної безпеки підприємства. Повна вартість володіння (TCO). Економічне обґрунтування (REJ). Інформаційна економіка (IE). Управління портфелем інформаційних активів. Вибір технічних засобів захисту інформації з урахуванням повної вартості володіння. Прикладна інформаційна економіка (AIE).

Тема 1.15. Створення підрозділу інформаційної безпеки

Ключові позиції відповідальності за інформаційну безпеку (CISO, BISO). Структура підпорядкованості. Профіль компетентності. Сертифікація CISO, функції CISO. Визначення чисельності підрозділу інформаційної безпеки. Набір, відбір, післядипломна освіта, навчання персоналу підрозділу інформаційної безпеки. Фінансування підрозділу інформаційної безпеки. Положення про структурні підрозділи, посадові інструкції. Відповідальність за порушення законодавства із захисту інформації з обмеженим доступом.

РОЗДІЛ 2.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тема 2.1. Закони України

«Про інформацію»; «Про державну таємницю»; «Про захист інформації в інформаційно-телекомунікаційних системах»; «Про надзвичайний стан»; Кримінальний кодекс України; Цивільний процесуальний кодекс України.

Тема 2.2. Державні стандарти України

ДСТУ 3396.0-96. Технічний захист інформації. Основні положення; ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт; ДСТУ 3396.2-97. Технічний захист інформації. Терміни та визначення; ДСТУ 3918-1999 (ISO/IEC 12207: 1995). Процеси життєвого циклу програмного забезпечення; ДСТУ ISO/IEC TR 13335-1:2003. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій; ДСТУ ISO/IEC TR 13335-2:2003. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки інформаційних технологій; ДСТУ ISO/IEC TR 13335-3:2003. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій; ДСТУ ISO/IEC TR 13335-4:2005. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту; ДСТУ ISO/IEC TR 13335-5:2005. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанова з керування мережною безпекою; Практичне застосування міжнародного стандарту ISO/IEC 17799:2005 «Управління інформаційною безпекою – Інформаційні технології».

Тема 2.3. Нормативні документи технічного захисту інформації

НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу; НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захисту оброблюваної інформації від несанкціонованого доступу. Положення про державну експертизу у сфері технічного захисту інформації.

Тема 2.4. Канали витоку інформації

Особливості витоку інформації. Характеристики технічних каналів витоку інформації. Класифікація каналів витоку інформації. Структура акустичного каналу витоку інформації. Характеристики акустичного каналу витоку інформації. Класифікація аудіоканалу витоку інформації. Структура радіоелектронного каналу витоку інформації. Характеристики радіоелектронних каналів витоку інформації. Класифікація радіоканалів витоку інформації. Структура оптичного каналу витоку

інформації. Характеристики оптичного каналу витоку інформації. Класифікація оптичних каналів витоку інформації.

Тема 2.5. Закладні пристрої

Структура закладних пристроїв. Класифікація закладних пристроїв. Закладні пристрої з передачею по радіоканалу. Закладні пристрої з передачею по провідним каналам.

Тема 2.6. Засоби перехоплення інформації

Структурна схема акустичного приймача. Класифікація та види мікрофонів. Аналогові диктофони. Цифрові диктофони. Структурна схема засобу перехоплення в оптичному діапазоні. Об'єктиви. Візуально-оптичні прилади. Фото- і кіноапарати. Засоби телевізійного спостереження. Відеомагнітофони. Прилади нічного бачення. Тепловізори. Структура типового комплексу перехоплення. Антени. Радіоприймачі

Тема 2.7. Виявлення закладних пристроїв

Демаскуючі ознаки закладних пристроїв. Класифікація засобів виявлення в локалізації закладних пристроїв. Індикатори поля. Апаратура радіоконтролю. Принципи контролю телефонних ліній та кіл електроживлення. Засоби придушення сигналів закладних пристроїв. Апаратура нелінійної локації. Виявники пустот, металодетектори та рентгенівські апарати. Способи та методи контролю приміщень на відсутність закладних пристроїв.

Тема 2.8. Програмно-апаратні пристрої захисту інформації

Захист від несанкціонованого доступу. Захист від копіювання. Захист від вірусів.

Тема 2.9. Основні способи захисту інформації технічними засобами

Класифікація методів захисту інформації. Охорона джерел інформації. Приховування інформації: інформаційне приховування, енергетичне приховування.

Тема 2.10. Апаратура захисту ліній зв'язку

Методи і засоби захисту телефонних ліній і апаратів. Засоби контролю телефонних ліній та апаратів. Технічні засоби виявлення телефонних радіоретрансляторів. Криптографічні методи та засоби захисту мовної інформації.

Тема 2.11. Засоби створення акустичних та електромагнітних маскуючих завад

Генератори шуму в акустичному діапазоні. Пристрої віброакустичного захисту. Пристрої ультразвукового захисту приміщень. Засоби просторового зашумлення. Засоби лінійного зашумлення. Засоби створення маскуючих завад в

комунікаційних мережах. Засоби створення маскуючи завад в мережах електроживлення. Багатофункціональні засоби захисту.

ЛІТЕРАТУРА

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В. Б.Толубко, С.В. Дорошенко: К.: ДУТ, 2015 - 298 с.
2. Анисимов А.А. Менеджмент в сфере информационной безопасности М.: БИНОМ. 2009.
3. Бармен Скотт. Разработка правил информационной безопасности М.: Издательский дом “Вильямс”, 2002.
4. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, - 340 с.
5. Гринберг А.С. и др. Защита информационных ресурсов государственного управления. М.: ЮНИТИ-ДАНА, 2003.
6. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.
7. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.
8. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.
9. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ. К.: Держспоживстандарт України, 2005.
10. ДСТУ ISO/IEC TR 13335-3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ. К.: Держспоживстандарт України, 2005.
11. ДСТУ ISO/IEC TR 13335-4:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Настанови з керування безпекою інформаційних технологій. К.: Держспоживстандарт України, 2005.
12. ДСТУ ISO/IEC TR 13335-5:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою. К.: Держспоживстандарт України, 2005.
13. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. – М.:Издательская группа “БЦД-пресс”,2006. –304 с
14. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Компания АйТи, 2006. – 400 с.
15. Петренко С.А., Симонов С.А. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи, 2004. - 384 с.
16. Конституція України / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради України, 1996. – № 30. – Ст. 141.
17. Про інформацію [Електронний ресурс] Закон України від 02.10.2002 р. № 2657-XII. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

18. Про державну таємницю [Електронний ресурс] Закон України від 21.09.1999 р. № 1079-XIV. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

19. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] Закон України від 05.10.1994 р. № 80/94-ВР. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

20. Про надзвичайний стан [Електронний ресурс] Закон України від 26.06.1992 р. № 2501-XII. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

21. Кримінальний кодекс України [Електронний ресурс] Закон України від 05.04.2001 р. № 2341-III. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

22. Цивільний процесуальний кодекс України [Електронний ресурс] Закон України від 18.03.2004 р. № 1618-IV. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

23. Базові поняття. Терміни та визначення : ДСТУ 2392-94. – [Чинний від 01 – 01 – 1995]. – К. : Держстандарт України, 1994. – IV. 89 с. – (Державний стандарт України).

24. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997 – 01 – 01]. – К.: Держстандарт України, 1995. – IV. 8 с. (Державний стандарт України).

25. Технічний захист інформації. Порядок проведення робіт : ДСТУ 3396.1-96. – [Чинний від 1997 – 01 – 07]. – К.: Держстандарт України, 1995. – IV. 11 с. (Державний стандарт України).

26. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97 – [Чинний від 1998 – 01 – 01]. – К.: Держстандарт України, 1995. – IV. 12 с. (Державний стандарт України).

27. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207: 1995) : ДСТУ 3918-1999 – [Чинний від 2000-07-01]. – К. : Держстандарт України, 2000. VI. 49 с. (Державний стандарт України).

28. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій : ДСТУ ISO/IEC TR 13335-1:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – IV. 17 с. – (Національний стандарт України).

29. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки інформаційних технологій : ДСТУ ISO/IEC TR 13335-2:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – IV. 16 с. – (Національний стандарт України).

30. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій : ДСТУ ISO/IEC TR 13335-3:2003. –[Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – V. 42 с. – (Національний стандарт України).

31. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту : ДСТУ ISO/IEC TR 13335-4:2005. – [Чинний від 2006 – 07 – 01]. – К. : Держспоживстандарт України, 2007. – XI. 56 с. – (Національний стандарт України).

32. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанова з керування мережною безпекою: ДСТУ ISO/IEC TR 13335-5:2005. –

[Чинний від 2006 – 07 – 01]. – К. : Держспоживстандарт України, 2007. – VII. 23 с. – (Національний стандарт України).

33. Нормативне забезпечення інформаційної безпеки / [Головань С. М., Петров О. С., Хорошко В. О. та ін.]. – К. : Державний університет інформаційно-комунікаційних технологій, 2008. – 533 с.

34. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 15 с. (Нормативний документ системи технічного захисту інформації).

35. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1.-003-99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 24 с. (Нормативний документ системи технічного захисту інформації).

36. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4-001-2000. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 20 с. (Нормативний документ системи технічного захисту інформації).

37. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 : НД ТЗІ 2.5-008-2002. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2002. – III. 25с. (Нормативний документ системи технічного захисту інформації).

38. Головань С. М. Вимоги до побудови моделі загроз інформаційних систем / С. М. Головань // Інформаційна безпека – 2009. – № 2 (2) – С. 77–84.

39. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / Н. А. Кузнецов, В. В. Кульба, Е. А. Миркин и др.; Ин-т проблем информ. РАН. – М.: Наука, Т. 1. – 2006. – 538 с.

40. Класифікація інформації / С. М. Головань, А. М. Давиденко, Л. М. Щербак [та ін] // Защита информации: Сб. науч. тр. Национального авиационного университета. – 2005. – Вып. 12. – С. 8 – 16.

41. Несанкціоноване використання інформації та відповідальність за ці дії / С. М. Головань, А. М. Давиденко, О. О. Мелешко [та ін.] // Моделювання та інформаційні технології. Зб. наук. праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. – 2005. – Вип. 35. – С. 3–7.

42. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 1. Несанкционированное получение информации. К.: Издательство Арий, 2008.

43. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 2. Информационная безопасность. К.: Издательство Арий, 2008.

44. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Издательство «Ось-89», 1998, - 336 с.

45. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Изд. Юниор, 2003. – 504с.

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Склад предметної комісії визначається наказом ректора Державного університету телекомунікацій від 25.07.2016 № 299 «Про створення предметної комісії з приймання вступних іспитів до аспірантури», робота комісії та порядок проведення вступного випробування регламентується Правилами прийому до аспірантури для здобуття наукового ступеня доктора філософії у Державному університеті телекомунікацій в 2016-2017 роках, яке ухвалено вченою Радою Державного університету телекомунікацій (Протокол № 5 від 7 грудня 2015 року).

Гарант освітньої програми -
Голова предметної комісії
доктор технічних наук, професор В.Л. Бурячок

Секретар приймальної комісії –
завідувач відділу організації планування підготовки
та атестації аспірантів та докторантів
доктор технічних наук, старший науковий співробітник Є.В. Гаврилко