

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ОРГАНІЗАЦІЇ ТА ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ
АВАРІЙНО-РЯТУВАЛЬНИХ РОБІТ

(назва кафедри)

ЗАТВЕРДЖУЮ

Ректор Національного університету
цивільного захисту України
д-р наук з держ. упр., професор

В.П. Садковий

«___» _____ 2017 р.

«ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

(назва навчальної дисципліни)

Програма

навчальної _____ вибіркової _____ дисципліни
(обов'язкової, вибіркової)

підготовки _____ бакалавр _____
(назва освітнього ступеня)

спеціальності _____ 263 «Цивільна безпека» _____
(шифр і назва спеціальності)

спеціалізації _____ «Телекомунікаційні системи в управлінні» _____

Харків 2017 рік

Розробник(и) програми:

Борисова Л.В. – доцент кафедри організації та технічного забезпечення аварійно-рятувальних робіт Національного університету цивільного захисту України, кандидат юридичних наук
(посада, науковий ступінь та вчене звання)

Програму навчальної дисципліни рекомендовано кафедрою
організації та технічного забезпечення аварійно-рятувальних робіт
(назва кафедри)

Протокол від «__» _____ 201_ року № __

Начальник (завідувач) кафедри організації та технічного забезпечення аварійно-рятувальних робіт
(назва кафедри)

_____ В.О. Собина
(підпис) (прізвище та ініціали)

«__» _____ 20__ року

Рекомендовано вченою радою факультету цивільного захисту
(назва факультету)

Протокол від «__» _____ 201_ року № __

Голова вченої ради факультету цивільного захисту
(назва факультету)

_____ М.М. Удянський
(підпис) (прізвище та ініціали)

«__» _____ 20__ року

Схвалено вченою радою університету _____

Протокол від «__» _____ 201_ року № __

ВСТУП

Програма вивчення обов'язкової навчальної дисципліни «Основи інформаційної безпеки» складена відповідно до освітньо-професійної програми підготовки бакалавра за спеціальністю 263 «Цивільна безпека» спеціалізації «Телекомунікаційні системи в управлінні» і належить до циклу професійної підготовки.

Предметом вивчення навчальної дисципліни є формування у курсантів знання:

- правового регулювання забезпечення інформаційних відносин та інформаційної безпеки;
- факторів та каналів уразливості інформації, основні методи, принципи, способи, алгоритми та протоколи захисту інформації;
- критеріїв та показників оцінки якості захисту інформації;
- основних каналів витоку інформації по технічних каналах та їх аналітичні моделі;
- стандартизації, уніфікації методів, способів, засобів і заходів забезпечення інформаційної безпеки інформаційної сфери;

Міждисциплінарні зв'язки: теоретичний та практичний матеріал дисципліни базується на основі вивчення таких дисциплін як «Вища математика», «Фізика», «Інформатика та комп'ютерна техніка». Дисципліна «Основи електрозв'язку» використовується при вивченні наступних дисциплін професійного та практичного напрямку: «Основи побудови телекомунікаційних систем та мереж», «Спеціалізовані телевізійні системи», «Технічне забезпечення та експлуатація телекомунікаційних систем та мереж», «Кінцеві засоби телекомунікаційних систем та мереж».

Програма навчальної дисципліни складається з модулів:

1. Інформаційна безпека в системі ДСНС України

1. Мета та завдання навчальної дисципліни

1.1. **Мета:** набуття здобувачами вищої освіти компетентностей, знань з використання теорії електричних кіл та умінь аналітично та експериментально досліджувати основні процеси, що відбуваються в електричних колах для здійснення професійної діяльності з технічного обслуговування телекомунікаційного, мережного обладнання та обладнання станційного електрозв'язку.

1.2. **Завдання:** вивчення моделей загроз інформації, яку захищають, методам забезпечення цілісності, конфіденційності, доступності, захищеності від несанкціонованих дій.

1.3. У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

знати:

- правове регулювання забезпечення інформаційних відносин та інформаційної безпеки;

- фактори та канали уразливості інформації, основні методи, принципи, способи, алгоритми та протоколи захисту інформації;
- критерії та показники оцінки якості захисту інформації;
- основні канали витоку інформації по технічних каналах та їх аналітичні моделі;
- стандартизацію, уніфікацію методів, способів, засобів і заходів забезпечення інформаційної безпеки інформаційної сфери;

вміти:

- розробляти моделі загроз безпеці інформації, вирішувати завдання аналізу та синтезу алгоритмів і протоколів захисту інформації;
- оцінювати захищеність від несанкціонованого доступу до інформації;
- обґрунтовувати вимоги до ключових даних, здійснювати аналіз їх властивостей;
- самостійно вирішувати практичні задачі щодо забезпечення безпеки інформаційних ресурсів і засобів їхньої обробки в єдиному інформаційному просторі;
- формулювати рекомендації щодо розробки механізму реалізації, науково-практичних пропозицій і рекомендацій з підвищення ефективності організаційного управління забезпеченням інформаційної безпеки;

бути ознайомленим з:

- питаннями правового регулювання інформаційних суспільних відносин, в тому числі відносин і сфері забезпечення інформаційної безпеки;
- досвідом діяльності по проведенню робіт, пов'язаних із захистом інформації та інформаційною безпекою.

1.4. Компетентності, якими повинен оволодіти здобувач вищої освіти: здатність обґрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності підрозділів цивільного захисту відповідно до вимог діючих стандартів та нормативних документів.

На вивчення навчальної дисципліни відводиться 120 годин / 4 кредитів ЕКТС.

2. Інформаційний обсяг дисципліни

Модуль № 1. Інформаційна безпека в системі ДСНС України

Становлення та розвиток захисту інформації в Україні.

Забезпечення інформаційної безпеки в системі ДСНС України: інформаційна безпека: поняття, структура, зміст; державна таємниця як особливий вид інформації, що захищається; забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій; організація діяльності підрозділів технічного захисту інформації в системі Державної служби України з надзвичайних ситуацій.

Загрози інформаційній безпеці: основні характеристики інформаційної системи як об'єкта захисту; класифікація загроз інформаційній безпеці; ієрархічна класифікація загроз інформаційній безпеці; джерела загроз інформаційній безпеці.

Захист інформації як інтегральна проблема та шляхи її вирішення: умови безпеки інформації; державна політика і система ТЗІ в Україні; нормативно-правова база України в сфері ТЗІ; структура системи захисту інформації.

Класифікація та характеристика технічних каналів витоку інформації: загальна характеристика технічного каналу витоку інформації; класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ.

Класифікація та характеристика технічних каналів витоку інформації (2): особливості витоку інформації технічними каналами; типова структура та види технічних каналів витоку інформації; класифікація методів та засобів захисту інформації від витоку технічними каналами.

Загальні методи забезпечення інформаційної безпеки України. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи; правові методи забезпечення інформаційної безпеки; організаційно-технічні методи забезпечення інформаційної безпеки; економічні методи забезпечення інформаційної безпеки; забезпечення інформаційної безпеки у загальнодержавних і телекомунікаційних системах.

Концепція інженерно-технічного захисту інформації: основні положення концепції інженерно-технічного захисту інформації; системний підхід до інженерно-технічного захисту інформації; основні положення системного підходу до інженерно-технічного захисту інформації; цілі, завдання та ресурси системи захисту інформації; загрози безпеки інформації й заходи для їхнього запобігання.

Методи і засоби захисту інформації в комп'ютерних системах: захист інформації в комп'ютерних системах від несанкціонованого доступу; захист інформації в розподілених системах.

Правові питання захисту інформації із використанням технічних засобів: особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів; правове регулювання захисту інформації в засобах зв'язку; правове

регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу.

4. Рекомендована література

4.1. Базова

Основоположні законодавчі акти:

1. Про державну таємницю [Текст]: Закон України від 21.01.1994 № 3855-ХІІ // Відомості Верховної Ради України. – 1994. – № 16. – ст. 93.
2. Про інформацію [Текст]: Закон України від 02.10.1992 № 2657-ХІІ // Відомості Верховної Ради України. – 1992. – № 48. – ст. 650.
3. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України № 440 від 12.08.2005 [Текст] // Офіційний вісник України. – 2005. – № 34. – ст. 2089.
4. Про електронний цифровий підпис [Текст]: Закон України від 22.05.2003 № 852-ІV // Відомості Верховної Ради України. – 2003. – № 36. – ст. 276.
5. Про електронні документи та електронний документообіг [Текст]: Закон України від 22.05.2003 № 851-ІV // Відомості Верховної Ради України. – 2003. – № 36. – ст. 275.
6. Про захист інформації в телекомунікаційних системах [Текст]: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – ст. 286.

Основна навчальна література:

7. Антонюк А.О. Основи захисту інформації в автоматизованих системах [Текст]: навчальний посібник / А.О. Антонюк. – К.: Вид. дім «КМ Академія», 2003. – 242 с.
8. Богуш В.М., Юдин О.К. Інформаційна безпека держави: навчальний посібник / В.М. Богуш, О.К. Юдин. – К.: «МК-Прес», 2005. – 432 с.
9. Завгородний В.И. Комплексная защита информации в компьютерных системах [Текст]: учебное пособие / В.И. Завгородний. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с.
10. Мельников, В.В. Защита информации в компьютерных системах [Текст] / В. В. Мельников – М.: Финансы и статистика; Электроинформ, 1997 – С.231–239.
11. Пилипчук В.Г., Дзьобань О.П., Настюк В.Я. Система і компетенція державних органів зі спеціальним статусом у сфері національної безпеки України [Текст]: монографія / В.Г. Пилипчук, О.П. Дзьобань, В.Я. Настюк. – Х.: Право, 2009. – 200 с.
12. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации [Текст]: учебное пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2001. – 304 с.
13. Стенг Д., Мун С. Секреты безопасности сетей [Текст] / Д. Стенг., С. Мун. – К.: Диалектика, 1995. – 544 с.

Додаткова література:

14. Зегжда П.Д. Теория и практика обеспечения информационной безопасности [Текст] / П.Д. Зегжда. – М.: Изд-во «Яхтсмен», 1996. – 192 с.
15. Цветков В.Я. Технологии и системы информационной безопасности: Аналит. обзор. [Текст] / В.Я. Цветков. – М.: ВНИИЦ, 2001. – 88 с.

4. Форма підсумкового контролю успішності навчання

У процесі вивчення дисципліни магістри виконують модульну роботу. Підсумковими формами контролю є екзамен у 4 семестрі.

Для оцінки знань магістрів використовується поточний та підсумковий контроль. Поточний контроль здійснюється на кожному практичному занятті методом фронтального опитування, тестування, письмової контрольної роботи, виконанням і захистом лабораторних робіт.

Розробник(и) програми:
доцент кафедри ОТЗАРР,
кандидат юридичних наук

(посада, вчене звання, ступінь)

(підпис)

Л.В. Борисова

(прізвище та ініціали)