# БЕЗПЕКА ПРОГРАМ ТА ДАНИХ (ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ)

*Академічна характеристика дисципліни*

| Рік вивчення (курс) | Семестр | Кількість кредитів ECTS | Кількість годин | | | | | | Кількість годин на тиждень | Форма підсумкового контролю | Система оцінювання |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | *Всього* | *Лекції* | *Лабораторні* | *Практичні* | *Семінарські* | *Самостійна робота* | | | |
| 4 | I | 4 | 144 | 24 | 34 | | | 86 | 4 | Іспит | 100-бальна, ECTS, національна (4-бальна) |

*Тип дисципліни* – нормативна.

*Викладач* – Супруненко Оксана Олександрівна, кандидат технічних наук, доцент.

*Мова вивчення* – українська.

*Форми організації освітнього процесу* – лекції, лабораторні заняття, самостійна робота, індивідуальні творчі завдання.

**Заплановані результати навчання:** У результаті вивчення дисципліни студент повинен:

- знати про потенційні загрози інформації і програмним системам у сучасних у комп‘ютерних мережах;
- знати та вміти цілеспрямовано використовувати правову та нормативну базу щодо порядку обробки, захисту та поширення інформації у комп‘ютерних мережах;
- знати технології оцінки рівня стійкості захисту ПЗ, складові політики безпеки сучасної організації;
- знати методи та засоби захисту інформації від зовнішніх загроз, в тому числі від хакерських атак, комп‘ютерних вірусів та іншого небезпечного програмного забезпечення;
- знати принципи та структуру систем захисту програмних систем від несанкціонованого доступу;
- знати методи криптографічного захисту від порушення конфідентцій-ності та цілісності інформації, як підґрунтя для створення підсистем захисту ПЗ, що реалізуються студентами на практиці;
- вміти аналізувати потенційні загрози при збереженні цілісності, доступності та конфіденційності інформації у комп‘ютерних мережах організації, та використовувати методи та засоби захисту програм та даних організації;
- вміти з реалізовувати елементи системи захисту від несанкціонованого доступу, в тому числі криптографічні засоби захисту інформації від порушення конфіденційності;

- мати навички захисту особистої інформації у мережі Internet;
- мати навички відстеження оперативної інформації про нові загрози безпеці інформації та програмним системам.

**Компетентності студента:**

- здатність цілеспрямовано використовувати правові та нормативні документи щодо порядку обробки, захисту та поширення інформації;
- вміння відстежувати та критично оцінювати інформаційні джерела про нові загрози безпеці інформації та програмними системам;
- спроможність встановлювати та аналізувати потенційні загрози збереженим даним та програмному забезпеченню, а також канали їх реалізації;
- здатність застосовувати способи, методи та засоби захисту програм та даних від загроз конфіденційності, цілісності та доступності;
- здатність створювати модулі захисту програм та даних із застосуванням сучасних методів криптографії;
- здатність формувати структуру системи захисту програмного продукту від несанкціонованого доступу та реалізовувати складові створеного проекту;
- здатність представляти та аргументовано обґрунтовувати реалізоване технічне рішення під час прилюдного захисту роботи.

**Змістові модулі (перелік тем):**

*Змістовий модуль 1. Основи безпеки інформації та програмного забезпечення*

*Тема 1.1.* Поняття про інформаційну безпеку. Правова та нормативна база щодо порядку обробки, захисту та поширення інформації.

*Тема 1.2.* Грані інформаційної безпеки, основні загрози та способи протидії. Об‘єктно-орієнтований підхід для забезпечення інформаційної безпеки. Заходи та засоби реалізації інформаційної безпеки. Політика безпеки.

*Тема 1.3.* Види хакерських атак. Основні небезпеки. DDoS-атаки, об‘єкти та способи протидії.

*Змістовий модуль 2. Комп’ютерні віруси та методи боротьби з ними*

*Тема 1.1.* Класифікація комп‘ютерних вірусів. Еволюція програмного забезпечення та комп’ютерних вірусів.

*Тема 1.2.* Особливості внесення комп‘ютерних вірусів. Антивірусний захист комп’ютеризованого робочого місця, програмні засоби та організаційні заходи.

*Тема 1.3.* Програмні засоби та організаційні заходи захисту мережевих систем. Профіль особистої інформаційної безпеки.

*Змістовий модуль 3. Технічний захист внутрішнього периметру*

*Тема 1.1.* Програмні та апаратно-програмі засоби захисту інформації. Структура системи захисту від несанкціонованого доступу.

*Тема 1.2.* Методи сучасної криптографії. Ідентифікація та аутентифікація. Парольний захист. Стійкі паролі, особливості реалізації парольного захисту.

*Тема 1.3.* Клавіатурні шпигуни (кейлогери), механізми їх функціонування, засоби захисту від кейлогерів.

*Тема 1.4*. Самовиліковне програмне забезпечення, структура, функції та перспективи впровадження.

**Рекомендована література**

***Основна:***


1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
2. Задірака В. К., Кудін А. М. та ін. Комп'ютерні технології криптографічного захисту інформації на спеціальних носіях: Навч. посіб. – К. – 2007. – 272 с.
3. Задірака В.К. Хмарні обчислення в криптографії та стеганографії / В.К. Задірака, А.М.Кудін // Кибернетика и сист. анализ. – 2013. – 49, №4. – С. 113-119.
4. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних. К.: - Вид-во ТОВ «НВП Інтерсервіс», 2009. – 713 с.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» - чинний з 05.07.1994 (зі змінами до 27.03.2014). [Електронний документ]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/80/94-вр. Перевірено 27.08.2017.
6. Закон України «Про захист персональних даних» – Чинний з 2010 р. (зі змінами до 2017). [Електронний документ]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17. Перевірено 27.08.2017.
7. Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» – Чинний з 2005 р. [Електронний документ]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2594-15. Перевірено 25.08.2017.
8. Указ президента «Про Положення про порядок здійснення криптографічного захисту інформації» - чинний з 1998 р. (зі змінами до 28.08.2009). [Електронний документ]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/505/98. Перевірено 27.08.2017.


***Додаткова:***


1. Кобозева А. А., Мачалін І. О., Хорошко В. О. Аналіз захищеності інформаційних систем. / Підручник. – К.: ДУІКТ, 2010. – 316 с.
2. Коваленко М.М. Комп'ютерні віруси і захист інформації. - Київ : Наукова думка, 1999.
3. Люцарев В.С. и др. Безопасность компьютерных сетей на основе Windows NT. – М.: Изд. отд. «Русская редакция» ТОО «Channel Trading Ltd.», 1998.
4. Гульев И. Компьютерные вирусы, взгляд изнутри.– М.: ДМК, 1998.–304 с.
5. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика - Электронинформ, 1997. – 364 с.
6. Касперски К. Техника и философия хакерских атак. – М.: СОЛОН – Р, 2001. – 272 с.
7. Касперски К. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005. – 316 с.
8. Корт С.С.. Теоретические основы защиты информации. – М.: Гелиос, АРВ, 2004.

9. Венбо Мао. Современная криптография: теория и практика, : Пер. с англ. – М. : Издательский дом «Вильямс», 2005. – 768 с.
10. Хореев О.В. Криптографические интерфейсы и их использование. – М.: Горячая линия – Телеком, 2007. – 278 с.
11. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций. – М.: Горячая линия – Телеком, 2008. – 346 с.
12. Стивен Норкатт и др. Защита сетевого периметра. Пер. с англ./ Под науч. ред. чл.-корр. Украинской Академии Информатизации Алишова Н.И. – К.: ООО ТИД «Диасофт», 2004. – 672 с.
13. Вильям Столингс. Криптография и защита сетей. – М.: Вильямс, 2001.
14. Лебедь С.В.. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: Издательство МГТУ имени Н.Э. Баумана, 2002.