**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**
**СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ**
**Система забезпечення якості освітньої діяльності та якості вищої освіти**
*сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015*
**Кафедра програмної інженерії та кібербезпеки**

**ЗАТВЕРДЖЕНО**
вченою радою
(пост. 10 п. 10 від "21" червня 2018 р.)
Ректор
_____ А.А. Мазаракі

# БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

## ПРОГРАМА ТА РОБОЧА ПРОГРАМА / SYLLABUS

| | |
|---|---|
| **освітній ступінь** | **магістр /** master |
| **галузь знань** | **12 Інформаційні технології /** Information Technology |
| **спеціальність** | **121 Інженерія програмного забезпечення /** Software Engineering |
| **спеціалізація** | **Інженерія програмного забезпечення /** Software Engineering |

**Київ 2018**

Автор: В.І. Пашорін, канд.техн.наук, проф.

Програму та робочу програму розглянуто і затверджено на засіданні кафедри програмної інженерії та інформаційних систем 15 травня 2018 р., протокол №26.

Рецензенти: Рзаєва С.Л., канд. техн. наук, доцент,
Бабенко Б.Т., технічний директор CIO, Softorino Inc.

# БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

## ПРОГРАМА ТА РОБОЧА ПРОГРАМА / SYLLABUS

| | |
|---|---|
| **освітній ступінь** | **магістр /** master |
| **галузь знань** | **12 Інформаційні технології /** Information Technology |
| **спеціальність** | **121 Інженерія програмного забезпечення /** Software Engineering |
| **спеціалізація** | **Інженерія програмного забезпечення /** Software Engineering |

**Автор: ПАШОРІН Валерій Іванович**

# ВСТУП

Одним із напрямків кібербезпеки є забезпечення захисту інтернет-ресурсів. Кількість інтернет-ресурсів (серверів різноманітного призначення та інфраструктури глобальних мереж) збільшується щороку, все ширше використовуються хмарні технології і віддалений доступ до ресурсів, а значить і зростає кількість інформації, яка локалізується на таких ресурсах і в глобальних мережах. Прагнення незаконно використовувати цю інформацію, спотворювати її, або умисно блокувати доступ до неї стимулює зростання атак на інтернет-ресурси, що приводить не тільки до економічних, а й політичних і соціальних наслідків. Атаки на державні та урядові інтернет-ресурси взагалі розглядається як елемент поширення гібридних війн у світі.

Таким чином, напрямок кібербезпеки, який стосується захисту інтернет-ресурсів, стає все більш актуальним, особливо з урахуванням постійного вдосконалення методів та інструментів атак. Дисципліна «Безпека інтернет-ресурсів» покликана надати більш детальний розгляд по цьому напрямку. Змістовна частина дисципліни включає вивчення сучасних методів та засобів захисту интернет-ресурсів. Як засоби для забезпечення безпеки інтернет-ресурсов використовуються: антивірусні програми, міжмережеві екрани, віртуальні приватні мережі (VPN), засоби мережевої аутентифікації, авторизації і шифрування, засоби захисту мережевих ресурсів на основі розмежування повноважень користувачів, засоби активного дослідження захищеності ресурсів, засоби попередження про мережеві атаки і засоби виявлення таких атак.

Програма та робоча програма складається з таких розділів:

1. Мета, завдання та результати вивчення (компетенції) дисципліни, її місце у освітньому процесі.
2. Зміст дисципліни.
3. Структура дисципліни та розподіл годин за темами (тематичний план).
4. Тематика та зміст лекційних, лабораторних занять, самостійної роботи студентів.
5. Список рекомендованих джерел.

## 1. МЕТА, ЗАВДАННЯ ТА РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ (КОМПЕТЕНТНОСТІ), ЇЇ МІСЦЕ в ОСВІТНЬОМУ ПРОЦЕСІ

**Метою** викладання дисципліни є формування теоретичних знань та практичних навичок необхідних для безпечного використання інтернет-ресурсів і безпечній роботі в глобальних мережах.

**Предметом** вивчення дисципліни є вивчення основних положень і принципів, покладених в безпеку функціонування інтернет-ресурсів, та програмних і технічних засобах що їх реалізують.

**Задачі вивчення** дисципліни полягають у тому, щоб ознайомити студентів і надати їм навички в роботі по установці, настройці, експлуатації і підтримки в працездатному стані системи захисту ітернет-реурсів і безпечній роботі при використані глобальних мереж.

В результаті вивчення дисципліни студент повинен:

**Знати:**
- вимоги нормативних документів України по безпеці в глобальних мережах;
- основні положення, організацію та моделі систем захисту інтернет-ресурсів;
- класифікацію атак на інтернет-ресурси та міри протидії;
- технологію та правила мережевої аутентифікації ресурсів і користувачів;
- організацію і правила безпеки при роботі в глобальних мережах;
- технологію та правила експлуатації міжмережевих екранів;
- основи технології віртуальних захищених мереж VPN;
- основи забезпечення захисту в мережевих протоколах передачі.

**Вміти:**
- визначати загрози інтернет-ресурсам;
- здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі;
- організувати захищений видалений доступ до інтернет-ресурсів;
- аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них;
- встановлювати і налагоджувати міжмережеві екрани;
- реєструвати порушення режиму безпеки і складати звіти;
- розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів;
- створювати захист за допомогою програмних засобів;

- організовувати безпечну роботу в глобальних мережах;
- використовувати VPN-рішення для побудови захищених мереж;
- управляти засобами безпеки інтеренет-ресурсів.

Вивчення дисципліни передбачає використання наступних видів занять: лекції, лабораторні роботи (в комп'ютерному класі на ПК), самостійна робота студентів. Підсумковий контроль проводиться у формі екзамену.

**Місце дисципліни в освітньому процесі.** Для опанування цією дисципліною за програмою достатньо знань, отримання яких передбачено у програмах Університету з вивчення дисциплін: «Вища математика», «Алгоритмізація та програмування», «Безпека програм та даних», «Методи і засоби захисту інформації в комп'ютерних системах».

## 2. ЗМІСТ ДИСЦИПЛІНИ

**Тема 1.** Основи мережевої безпеки

Розподілені ресурси: механізми безпеки і управління. Мережева безпека: терміни та визначення. Нормативні документи по безпеці в глобальних мережах. Стандарти безпеки мереж і їх компонентів. Класифікація мережевих загроз та атак на інтернет-ресурси. Технології виявлення віддалених атак. Соціальна інженерія. Шляхи вирішення проблем захисту інтернет-ресурсів.

**Список рекомендованих джерел:**
Основний: 4,6,7,8
Додатковий: 12, 13

**Тема 2.** Технології фільтрації мережевого трафіку

Фільтрація трафіку. Фільтрація Web-змісту (WCF). Віртуальні локальні мережі (VLAN). Технологія перетворення мережевих адрес (NAT). Міжмережеві екрани (МЕ): класифікація та функції МЕ. Варіанти виконання МЕ. Схеми мережевого захисту на базі МЕ. Основні схеми підключення МЕ. Персональні і розподілені мережеві екрани. Довірена мережа та DMZ мережі. Формування політики міжмережевої взаємодії. Проблеми безпеки МЕ.

**Список рекомендованих джерел:**
Основний: 4,5,6,7,8
Додатковий:11, 12

**Тема 3.** Основи технології віртуальних приватних мереж

Концепція побудови віртуальних приватних мереж VPN. Основні поняття і функції мережі VPN. Варіанти побудови віртуальних захищених каналів. Засоби забезпечення безпеки VPN. VPN-рішення для побудови захищених мереж. Класифікація мереж VPN. Основні варіанти архітектури VPN.

**Список рекомендованих джерел:**
Основний: 4,5,6,7
Додатковий: 11,12,13

**Тема 4.** Протоколи мережевої безпеки

Протоколи захисту інтеренет-ресурсів на канальному рівні (протокол PPTP, L2TP). Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS) . Захист інтернет-ресурсів на мережевому рівні (протокол IPSec). Особливості реалізації засобів IPSec.

Основні схеми застосування IPSec . Протоколи захисту у безпроводних мережах. Механізм шифрування WEP. Специфікація WPA. Стандарт мережі з підвищеною безпекою WPA2.

**Список рекомендованих джерел:**
Основний: 4,5,7
Додатковий: 11,12

**Тема 5.** Безпека інтернет-ресурсів на прикладному рівні

Управління мережевою ідентифікацією і доступом. Особливості управління доступом. Функціонування системи управління доступом. Організація захищеного видаленого доступу. Протоколи аутентифікації видалених користувачів. Централізований контроль видаленого доступу. Протокол Kerberos. Інфраструктура управління відкритими ключами PKI.

**Список рекомендованих джерел:**
Основний: 4,5,6,7,10
Додатковий: 11,12

**Тема 6.** Аналіз безпеки інтернет-ресурсів

Концепція адаптивного управління безпекою. Технологія аналізу захищеності. Засоби аналізу захищеності мережевих протоколів і сервісів. Технології виявлення атак. Класифікація систем виявлення атак IDS. Компоненти і архітектура IDS. Системи попередження атак IPS. Методи реагування систем на атаки. Безпечне розгортання сервісів DNS. Безпека Web-серверів. Безпечна мережева інфраструктура для Web-сервера.

**Список рекомендованих джерел:**
Основний: 4,5,6,7
Додатковий: 11,13

## 3. СТРУКТУРА ДИСЦИПЛІНИ ТА РОЗПОДІЛ ГОДИН ЗА ТЕМАМИ (ТЕМАТИЧНИЙ ПЛАН)

| *Назва теми* | *Кількість годин* | | | | *Форми контролю* |
|---|---|---|---|---|---|
| | *Усього годин/кредитів* | *За формами занять* | | | |
| | | *Лекції* | *Лабораторні заняття* | *Самостійна робота студентів* | |
| **Тема 1.** Основи мережевої безпеки | 12 | 2 | 4 | 24 | УО ІЗ |
| **Тема 2.** Технології фільтрації | 12 | 4 | 8 | 38 | УО |

| | | | | | |
|---|---|---|---|---|---|
| мережевого трафіку | | | | | Пр |
| **Тема 3.** Основи технології віртуальних приватних мереж | 14 | 2 | 4 | 24 | УО, ІЗ, Пр |
| **Тема 4.** Протоколи мережевої безпеки | 70 | 2 | 4 | 24 | УО, ІЗ, Пр |
| **Тема 5.** Безпека інтернет-ресурсів на прикладному рівні | 36 | 2 | 4 | 24 | ІЗ, Пр |
| **Тема 6.** Аналіз безпеки інтернет-ресурсів | | 2 | 4 | 24 | |
| **Разом** | **180/6** | **14** | **28** | **158** | |
| **Підсумковий контроль семестру - екзамен** | | | | | |

Умовні позначення:

УО – усне опитування ІЗ – перевірка індивідуальних завдань

ПО – письмове опитування Т – тестування

Пр. – презентація індивідуального завдання

## 4. ТЕМАТИКА ТА ЗМІСТ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ* ЗАНЯТЬ, САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

| *Результати навчання* | *Навчальна діяльність** | *Робочий час студента год* | *Оцінювання у балах* |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **SoftSkills:** комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики. | **Тема 1. Основи мережевої безпеки** | | |
| **Знати:** основні положення, організацію та моделі систем захисту інтернет-ресурсів; класифікацію атак на інтернет-ресурси та міри протидії | **Лекція 1. План лекції**<br>1. Розподілені ресурси: механізми безпеки і управління<br>2. Мережева безпека: терміни та визначення<br>3. Класифікація мережевих загроз та атак на інтернет-ресурси<br>4. Шляхи вирішення проблем захисту інтернет-ресурсів<br>**Список рекомендованих джерел**<br>Основний: 2, 3, 4<br>Додатковий: 10, 11 | 2 | |
| **Вміти:** здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції з питань:<br>1. Нормативні документи по безпеці в глобальних мережах<br>2. Технології виявлення віддалених атак<br>3. Соціальна інженерія | 24 | 2 |
| **Вміти:** здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі | **Лабораторна робота № 1**<br>*Засоби мережного аудиту*<br>Завдання на лабораторну роботу:<br>1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи<br>2.Запустити утиліту TCPView. Ознайомтеся з основними пунктами меню<br>3. Занести до протоколу результати сканування відкритих з'єднань<br>4. Відкрийте утиліту XSpider. Вивчіть основні пункти меню, скориставшись документацією з меню «Довідка»<br>5. Запустити програму сканування<br>6. Виконати сканування по окремих сервісах<br>7. Проаналізуйте результати сканування | 4 | 8 |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | вашого завдання. Занесіть до звіту результат сканування.<br>8. Занесіть до звіту порівняльну характеристику, отриманих вами результатів за допомогою утиліт TCPView і XSpider | | |
| **SoftSkills:** комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент | **Тема 2. Технології фільтрації мережевого трафіку** | | |
| **Знати:** технологію та правила експлуатації міжмережевих екранів | **Лекція 2. План лекції**<br>1. Фільтрація трафіку. Фільтрація Web-змісту (WCF)<br>2. Віртуальні локальні мережі (VLAN). Технологія перетворення мережевих адрес (NAT)<br>3. Міжмережеві екрани (МЕ): класифікація та функції МЕ<br>**Список рекомендованих джерел:**<br>Основний: 2-7<br>Додатковий: 10 | 2 | |
| **Вміти:** встановлювати і налагоджувати міжмережеві екрани | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції:<br>1. Варіанти виконання МЕ<br>2. Персональні і розподілені мережеві екрани<br>3. Основні схеми підключення МЕ | 20 | 4 |
| **Знати:** технологію та правила експлуатації міжмережевих екранів | **Лекція 3. План лекції**<br>1. Схеми мережевого захисту на базі МЕ<br>2. Довірена мережа та DMZ мережі<br>**3.** Формування політики міжмережевої взаємодії<br>**Список рекомендованих джерел:**<br>Основний: 2-7<br>Додатковий: 8,9,10 | 2 | |
| **Вміти:** аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань:<br>1. Проблеми безпеки МЕ<br>2. Інтерфейс та функціональні можливості програми Outpost Firewall. | 18 | 4 |
| **Вміти:** встановлювати і | **Лабораторна робота № 2**<br>*Організація мережевої безпеки за допомогою* | 4 | 8 |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| налагоджувати міжмережеві екрани | *міжмережевого екрана Outpost Firewall*<br><br>**Завдання на лабораторну роботу:**<br>1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи<br>2. Запустити програму Outpost Firewall. Вивчите функціональні можливості вкладок контекстного меню «Параметри»<br>3. Налаштувати функції програми Outpost Firewall, залежно від вимог, зазначених у варіанті<br>4. Налаштувати журнал програми Outpost Firewall, для відображення тільки необхідної інформації, обумовленої завданням<br>5. Підготувати звіт за результатами роботи програми й виконаними налаштуваннями | | |
| **Вміти:** аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них | **Лабораторна робота № 3**<br>*Організація мережевої безпеки при використанні засобів виявлення мережевих атак*<br>**Завдання на лабораторну роботу:**<br>1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи<br>2. Запустити утиліту APS, для виявлення факту сканування портів по протоколах TCP, UDP і розсилання UDP broadcast пакетів для заданих портів<br>3. Налаштувати утиліту APS за наданим варіантом<br>4. Налаштувати системи імітації сервісів TCP<br>5. Підготувати звіт за результатами роботи програми й виконаними налаштуваннями | 4 | 8 |
| **SoftSkills***:* комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент | **Тема 3. Основи технології віртуальних приватних мереж** | | |
| **Знати:** основи технології віртуальних захищених мереж VPN | **Лекція 4. План лекції**<br>*Концепція побудови віртуальних приватних мереж VPN*<br>1. Основні поняття і функції мережі VPN<br>2. Варіанти побудови віртуальних захищених каналів<br>3. Класифікація мереж VPN | 2 | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | 4. Основні варіанти архітектури VPN<br>**Список рекомендованих джерел:**<br>Основний: 3,4,5<br>Додатковий: 9,10 | | |
| **Вміти:**<br>використовувати VPN-рішення для побудови захищених мереж;<br>захищати за допомогою програмних засобів | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань:<br>1. Засоби забезпечення безпеки VPN Методи вкладення інформації у комп'ютерні файли<br>2. VPN-рішення для побудови захищених мереж | 24 | 2 |
| **Вміти:**<br>використовувати VPN-рішення для побудови захищених мереж;<br>захищати за допомогою програмних засобів | **Лабораторна робота 4**<br>*Організація мережевої безпеки при використанні засобів VPN*<br>**Завдання на лабораторну роботу:**<br>1. Встановити та підготувати віртуальну машину з ОС Windows 7 для виконання лабораторної роботи<br>2. Використовуючи **Центр управления сетями и общим доступом** створити нове з'єднання і налаштувати VPN тунель<br>3. Встановити та підготувати віртуальну машину з ОС Windows 10 для виконання лабораторної роботи<br>4. Використовуючи аплет **Мережі та Інтернет** створити VPN підключення<br>5. Встановити та налаштувати VPN –сервіс за варіантом<br>6. Підготувати звіт про виконання лабораторної роботи | 4 | 8 |
| **SoftSkills:**<br>комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент | **Тема 4. Протоколи мережевої безпеки** | | |
| **Знати:**<br>основи забезпечення захисту в мережевих протоколах передачі | **Лекція 5. План лекції**<br>*Протоколи захисту інтеренет-ресурсів*<br>1. Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS)<br>2. Захист інтернет-ресурсів на мережевому рівні (протокол IPSec) | 2 | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | 3. Особливості реалізації засобів IPSec<br>4. Протоколи захисту у безпроводових мережах<br>**Список рекомендованих джерел:**<br>Основний: 2,4,5,6<br>Додатковий: 9,12 | | |
| **Вміти:** організовувати безпечну роботу в глобальних мережах | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань:<br>1. Стандарт мережі з підвищеною безпекою WPA2<br>2. Основні схеми застосування IPSec | 24 | 2 |
| **Вміти:** організовувати безпечну роботу в глобальних мережах | **Лабораторна робота 5**<br>*Організація шифрування трафіку при використанні утиліти IPSec*<br>**Завдання на лабораторну роботу:**<br>1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи<br>2. Запустити консоль керування IPSec на комп'ютері<br>3. Створити свій список фільтрів, зазначений, залежно від варіанта<br>4. Створити власну дію фільтра, зазначену, залежно від варіанта<br>5. Створити свою політику IPSec<br>6. Додати до створеної політики, правило за зазначеними критеріями, залежно від варіанта<br>7. Підготувати звіт про виконання лабораторної роботи | 4 | 8 |
| **SoftSkills***:* комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент | **Тема 5. Безпека інтернет-ресурсів на прикладному рівні** | | |
| **Знати:** технологію та правила мережевої автентифікації ресурсів і користувачів | **Лекція 6. План лекції**<br>*Управління мережевою ідентифікацією і доступом*<br>1. Захищений віддалений доступ до мережі<br>2. Функціонування системи управління доступом. Протоколи автентифікації віддалених користувачів<br>**3.** Централізований контроль доступу. Протокол Kerberos | 2 | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | **Список рекомендованих джерел:**<br>Основний: 5,6<br>Додатковий: 8,9 | | |
| **Вміти:** розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань:<br>1. Особливості управління віддаленим доступом | 24 | 6 |
| **Вміти:** розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів | **Лабораторна робота 6**<br>*Організація безпеки механізму мережевої автентифікації*<br>**Завдання на лабораторну роботу:**<br>1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи<br>2. Встановити та запустити програму . Cain&Abel. Ознайомитись з можливостями основних пунктів меню програми<br>3. Виконати сканування MAC-адрес робочих станцій у локальній мережі<br>4. Виконати завдання за варіантом<br>5. Підготувати звіт про виконання лабораторної роботи | 4 | 8 |
| **SoftSkills***:* комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент | **Тема 6. Аналіз безпеки інтернет-ресурсів** | | |
| **Знати:** організацію і правила безпеки при роботі в глобальних мережах | **Лекція 7. План лекції**<br>*Концепція адаптивного управління безпекою*<br>1. Технології виявлення атак. Класифікація систем виявлення атак IDS<br>2. Компоненти і архітектура IDS<br>3. Системи попередження атак IPS Методи реагування систем на атаки.<br>4. Безпека Web-серверів<br>**Список рекомендованих джерел:**<br>Основний: 5,6<br>Додатковий: 8,9 | 2 | |
| **Вміти:** створювати захист за | **Самостійна робота студентів**<br>Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: | 24 | 8 |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| допомогою програмних засобів; організовувати безпечну роботу в глобальних мережах | 1. Засоби аналізу захищеності мережевих протоколів і сервісів<br>2. Безпечна мережева інфраструктура для Web-сервера | | |
| **Вміти:** створювати захист за допомогою програмних засобів; організовувати безпечну роботу в глобальних мережах | **Лабораторна робота 7**<br>**Завдання на лабораторну роботу:**<br>1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи<br>2. Встановити та запустити програму *ESET Smart Security*. Ознайомитись з можливостями основних пунктів меню програми<br>3. Виконати налаштування сервісів програми за варіантом<br>4. Підготувати звіт про виконання лабораторної роботи | 4 | 8 |
| ***Разом за семестр*** | | ***180*** | ***100*** |

*Всі лабораторні роботи проходять в лабораторії кібербезпеки з використанням сучасних програмних засобів.

## 5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ*

### Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99

2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник Чернівці.- Видавничий дом «Родовід», 2017. – 471с.

3. Кавун С.В. Інформаційна безпека. Навчальний посібник Харків: ХНЕУ, 2016. -213с.

4. Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль – К., 2015. – 435 с., іл.160.

*5. Зубок М. І. Інформаційна безпека : Навчальний посібник для студентів вищих навч.закладів / М. І. Зубок. – К. : КНТЕУ, 2009. – 132с.*

*6. КавунС. В. Інформаційна безпека підручник / С. В. Кавун. – Харків : ХНЕУ, 2016. – 368с.*

7. Єсін В. І. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х.: ХНУ імені В. Н. Каразіна, 2015. – 632с.

### Додатковий

8. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.

9. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.

10. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.

*11. Кормич Б. А. Інформаційна безпека:організаційно-правові основи: навч. посібник для студентів вузів / Б. А. Кормич. – К. : Кондор, 2015. – 384с.*

*12. Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*

*13. Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*

### Internet-ресурси

*14.* Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*

15. Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*

*16.* Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*

* Курсивом виділені назви видань, які знаходяться в бібліотеці КНТЕУ.