КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ / SOFTWARE SECURITY

SYLLABUS

ОП 2018

освітній ступінь	**бакалавр**	**/**	bachelor
галузь знань	**12 Інформаційні технології**	/	Information technologies
спеціальність	**125 Кібербезпека**	/	Cybersecurity
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці**	/	Security of information and communication systems in the economy

Київ 2021

Автори: Ю.О. САМОЙЛЕНКО, канд. техн. наук, доцент

Силабус розглянуто і затверджено на засіданні кафедри програмної інженерії та інформаційних технологій 27 серпня 2021 протокол № 1.

СИЛАБУС

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ / SOFTWARE SECURITY

SYLLABUS

освітній ступінь	**бакалавр**	**/**	bachelor
галузь знань	**12 Інформаційні технології**	/	Information technologies
спеціальність	**125 Кібербезпека**	/	Cybersecurity
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці**	/	Security of information and communication systems in the economy

1. **Викладач**:

1.1. **Лектор**: Самойленко Юлія Олександрівна,

- *вчене звання та посада*: кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
- *педагогічний стаж* – 12 років;
- *e-mail:* y.samoilenko@knute.edu.ua ;
- *наукові інтереси*: інформаційні технології, інтелектуальні системи, інформаційні системи, комп'ютерні мережі, кібербезпека, WEB-технології
- *стажування та підвищення кваліфікації*:
  - Introduction to Cybersecurity. Cisco Networking Academy. 2020 р
  - IT Ukraine Association «Teacher's Internship program held by EPAM Systems» (липень – серпень 2021 р., 108 годин, сертифікат № 619)

2. **Дисципліна**: «**Безпека програмного забезпечення**»,
   - рік навчання: 4;
   - семестр навчання: 7;
   - кількість кредитів: 6;
   - кількість годин за семестр: 180 год.
     - лекційних: 24 год.
     - практичних: 48 год.
     - на самостійне опрацювання: 108 год.
   - кількість аудиторних годин на тиждень:
     - лекційних: 2 год.
     - лабораторних: 4 год.
3. **Час та місце проведення:**
   - аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни передбачено в аудиторіях: 510;
   - поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
   - всі лабораторні завдання виконуються на основі інтерактивних методів навчання у електронному середовищі. Передбачається можливість проведення практичних та лекційних занять на базах підприємств-партнерів.
   - під час карантинних обмежень усі заняття проводяться у Microsoft Teams, події плануються заздалегідь, повідомлення про заплановані події надсилається на корпоративну пошту, відображається у календарі та у команді БПЗ, лекції.
4. **Пререквізити та постреквізити навчальної дисципліни:**
   - **пререквізити:** дисципліна базується на знаннях та компетентностях, що набуває здобувач вищої освіти під час вивчення дисциплін «Основ кібербезпеки», «Безпека операційних систем».
   - **постреквізити:** Дисципліна надає студентам необхідні знання та навички, які будуть корисні при проходженні виробничої практики, підготовці до випускного кваліфікаційного проекту та у подальшій професійній діяльності.

- **програмні результати навчання та компетенці:** Відображені в освітній програмі та програмі дисципліни.

5. Результати вивчення дисципліни:

«Безпека програмного забезпечення»

«Безпека інформаційних і комунікаційних систем в економіці» (ОС бакалавр 2020 р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ1	Здатність застосовувати знання у практичних ситуаціях	1-10
КЗ4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	1-10
КЗ5	Здатність до пошуку, оброблення та аналізу інформації.	1-10
Фахові компетентності за освітньою програмою		
КФ5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	1-10
КФ12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	1-10
Програмні результати навчання за освітньою програмою		
14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	1-10
16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.	1-10
17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних	1-10
	архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.	
19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	1-10
20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації	1-10

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	
21	Вирішувати задачі забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	1-10
27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	1-10
28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	1-10
34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	1-10
36	Виявляти небезпечні сигнали технічних засобів.	1-10

6. Характеристика дисципліни:

6.1. Призначення навчальної дисципліни: Дисципліна «Безпека програмного забезпечення» є важливою складовою підготовки сучасних фахівців різних профілів. Вона є багатогранною та досить широкою, але з її допомогою можна суттєво підвищити свою конкурентоздатність на ринку праці.

6.2. Мета вивчення дисципліни: метою вивчення дисципліни «Безпека програмного забезпечення» є формування у майбутніх фахівців необхідного рівня знань щодо сучасних стандартів, підходів, методів та засобів захисту програмного забезпечення, що забезпечить конкурентоспроможність випускників університету на ринку праці і сприятиме успішній роботі в різних областях сучасного бізнесу.

6.3. Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

Назва теми	Кількість годин				Форми контролю
	Усього год/кредитів	Лекції	Лабораторні заняття	Самостійна робота студ.	
Тема 1. Введення в надійність та безпеку програмного забезпечення	15	2	4	9	УО, ЛР,
Тема 2. Загрози надійності та безпеки програмного забезпечення	15	2	4	9	УО, ЛР
Тема 3. Загальний огляд систем захисту програмного забезпечення	15	2	4	9	УО, ЛР,
Тема 4. Сучасний стан засобів подолання систем захисту	15	2	4	9	УО, ЛР

Тема 5. Захист від несанкціонованого копіювання	15	2	4	9	УО, ЛР
Тема 6. Загальні принципи захисту програм від несанкціонованого дослідження	15	2	4	9	УО, ЛР
Тема 7. Захист від дизасемблювання	15	2	4	9	УО, ЛР, Т
Тема 8. Захист від несанкціонованого налагодження	13	2	4	7	УО, ЛР
Тема 9. Криптографічні методи захисту від шкідливих програм	17	2	4	11	УО, ЛР
Тема 10. Технологія захисту від шкідливих програм	12	2	4	6	УО, ЛР
Тема 11. Засоби зламу систем захисту	18	2	4	12	УО, ЛР
Тема 12. Захист інформації у комп'ютерних мережах	15	2	4	9	УО, ЛР, Т
Разом	**180/6**	**24**	**48**	**108**	
Підсумковий контроль – екзамен					

УО – усне опитування; ЛР – захист лабораторних робіт; Т – тестування.

6.4. План вивчення дисципліни:

ТЕОРЕТИЧНИЙ БЛОК:

Навчальна діяльність	Робочий час студента (год.)
1	2
Тема 1. Ведення в надійність та безпеку програмного забезпечення *План лекції* 1. Види програмного забезпечення 2. Функціональна надійність програмного забезпечення в інформаційних системах 3. Поняття загальної надійності в інформаційних системах 4. Відмовобезпека та кібербезпека інформаційних систем 5. Взаємозв'язок функціональної та інформаційної безпеки критично важливих систем **Список рекомендованих джерел:** *Основний:* 1. *Додатковий:* 9, 10, 11, 12. *Інтернет-ресурси:* 30.	2
Тема 2. Загрози надійності та безпеки програмного забезпечення *План лекції* 1. Вразливості програмного забезпечення 2. Помилки у програмному забезпеченні 3. Характерні недоліки програм, що експлуатуються 4. Шкідливі програми **Список рекомендованих джерел:** *Основний:* 1.	2

1	2
Додатковий: 14, 15, 21, 22. *Нормативний:* 25, 27.	
Тема 3. Загальний огляд систем захисту програмного абезпечення *План лекції* 1. Мета та доцільність використання систем захисту 2. Класифікація систем захисту 3. Основні алгоритми систем захисту програмного забезпечення 4. Показники застосованості та критерії оцінювання систем захисту програмного забезпечення 5. Основні вимоги до розробки систем захисту програмного забезпечення 6. Розповсюджені типи захистів та їх недоліки **Список рекомендованих джерел:** *Основний:* 3. *Додатковий:*24	2
Тема 4. Сучасний стан засобів подолання систем захисту *План лекції* 1. Проблема існування засобів зламу захистів програмного забезпечення 2. Класифікація засобів подолання систем захисту програмного забезпечення 3. Програми розпакування, дешифрування та криптоаналізу **Список рекомендованих джерел:** *Основний:* 3, 4 *Додатковий:* 6, 7, 8, 9.	2
Тема 5. Захист від несанкціонованого копіювання *План лекції* 1. Методи розповсюдження програмного забезпечення. 2. Технології захистів програмного забезпечення. 3. Основні поняття операційної системи, необхідні для створення систем захисту. 4. Доступ до файлової системи операційної системи. 5. Захист програмного забезпечення методом прив'язки до комп'ютера. 6. Електронні ключі захисту. 7. Ведення обмежень на використання програмного забезпечення. **Список рекомендованих джерел:** *Основний:* 2, 3, 4 *Додатковий:* 18	2
Тема 6. Загальні принципи захисту програм від несанкціонованого дослідження *План лекції* 1. Принципи побудови систем захисту та їх функції. 2. Основні методи та засоби дослідження програм. 3. Способи вбудованих захисних механізмів в програмному забезпечені. 4. Структура програм, захищених від дослідження. **Список рекомендованих джерел:** *Основний*: 3, 4, 5. *Додатковий*: 10, 13, 20.	2
Тема 7. Захист від дизасемблювання *План лекції* 1. Необхідність та доцільність захисту від дизасемблювання. 2. Основні методи протидії дизасемблюванню програм.	2

1	2
3. Шифрування коду. 4. Маніпулювання EXE – заголовком. 5. Захист програм шляхом обфускації. 6. Способи реалізації ускладнення логіки. 7. Додаткові методи боротьби з автоматичними та інтерактивними дизасемблерами. **Список рекомендованих джерел:** *Основний:* 3, 5. *Додатковий:* 16, 18. *Нормативний:* 25, 27.	
Тема 8. Захист від несанкціонованого налагодження *План лекції* 1. Огляд та класифікація налагоджувачів. 2. Захист від налагоджувачів реального режиму. 3. Боротьба з налагоджувачами захищеного режиму. 4. Додаткові прийоми антиналагоджувального програмування. **Список рекомендованих джерел:** *Основний:* 3, 5. *Додатковий:* 12, 15, 20.	2
Тема 9. Криптографічні методи захисту від шкідливих програм *План лекції* 1. Методи автентифікації. 2. Методи забезпечення цілісності програм. 3. Класифікація криптоалгоритмів. Криптоаналіз. 4. Шифрування даних за допомогою спеціальних програм та утиліт. **Список рекомендованих джерел:** *Основний:* 1, 5. *Додатковий:* 16, 24. *Нормативний:* 25, 27.	2
Тема 10. Технологія захисту від шкідливих програм *План лекції* 1. Класифікація шкідливих програм. 2. Цикл функціонування вірусів. 3. Маровіруси. 4. Поштові віруси. 5. Спам і боротьба з ним. 6. Типи антивірусних програм. Захист від шкідливих програм. **Список рекомендованих джерел:** *Основний:* 1, 3, 5. *Додатковий:* 12, 14, 24	2
Тема 11. Особливості зламу автоматизованих систем та програмного забезпечення *План лекції* 1. Поняття та характеристика програмних засобів, призначених для незаконного проникнення в автоматизовану систему. 2. Атаки на автоматизовані системи в глобальній інформаційній мережі Internet. 3. Використання програмних закладок для зламу автоматизованих систем.. **Список рекомендованих джерел:** *Основний:* 1, 3, 5.	2

1	2
Додатковий: 12, 14, 24.	
Тема 12. Захист інформації у комп'ютерних мережах *План лекції* 1. Мережеві компоненти, що атакуються. 2. Сервери. Робочі станції. 3. Середовище передачі інформації. 4. Вузли комутації мереж. 5. Захист інформації при застосуванні особистої системи мережевого захисту. **Список рекомендованих джерел:** *Основний:* 3, 5. *Додатковий:* 12, 14, 24.	2

ЛАБОРАТОРНІ ЗАНЯТТЯ:

Навчальна діяльність	Робочий час студента (год.)

1	2
Тема 1. Ведення в надійність та безпеку програмного забезпечення ***Список рекомендованих джерел:*** *Основний:* 1. *Додатковий:* 9, 10, 11, 12. *Інтернет-ресурси:* 30. Лабораторне заняття № 1 **Захист операційної системи WINDOWS 10** **Мета:** Засвоїти принципи та технології захисту інформації в операційній системі Windows 10 за допомогою служби «Безпека у Windows» **Завдання**: Опрацювати теоретичні відомості до лабораторного заняття. Навчитись створювати локальний обліковий запис користувача чи адміністратора. Розуміти на налаштовувати функції служби «Безпека у Windows» **Результати навчання.** Знати предмет та завдання дисципліни, поняття надійності та безпеки програмного забезпечення. Знати налаштовувати функції служби «Безпека у Windows».	4
Тема 2. Загрози надійності та безпеки програмного забезпечення ***Список рекомендованих джерел:*** *Основний:* 1. *Додатковий:* 14, 15, 21, 22. *Нормативний:* 25, 27. Лабораторне заняття № 2 **Захист від фішингових схем в Microsoft Office** **Мета:** Засвоїти принципи й елементи технології захисту інформації в Microsoft Office від фішингових схем. **Завдання:** Опрацювати теоретичні відомості до лабораторного заняття. Ознайомитися з рівнями захисту комп'ютера від фішингових схем, установленням та зняттям повідомлень про фішингові атаки. Проаналізувати останні фішингові дослідження з сайту на веб-вузлі Anti-Phishing Working Group.	4

1	2
Результати навчання. Знати теоретичні основи захисту від фішингових схем. Знати рівні захисту комп'ютера від фішингових схем.	
Тема 3. Загальний огляд систем захисту програмного забезпечення ***Список рекомендованих джерел:*** *Основний:* 3. *Додатковий:*24 Лабораторне заняття № 3 **Захист інформації у Microsoft Word** **Мета:** Засвоїти принципи й елементи технології захисту інформації в Microsoft Word. **Завдання:** Опрацювати теоретичні відомості. Ознайомитися із рівнями захисту документа та його елементів порядком створення сертифікату та його приєднання до документа. Установити дозволи на внесення приміток і записаних виправлень, паролю для файлу, паролю для відкриття та зміну документа. **Результати навчання** Знати принципи та елементи захисту інформації у Microsoft Word.	4
Тема 4. Сучасний стан засобів подолання систем захисту ***Список рекомендованих джерел:*** *Основний:* 3, 4 *Додатковий:* 6, 7, 8, 9. Лабораторне заняття № 4 **Захист інформації в Microsoft Excel** **Мета:** Засвоїти принципи й елементи технології захисту інформації у Microsoft Excel **Завдання:** Встановити пароль на книгу. Встановити блокування окремих комірок. Розблокувати комірки захищеного листа. Встановити захист структури й вікон книги. Захистити елементи загальної книги. Створити макрос та встановити параметри безпеки. Створити цифровий сертифікат. **Результати навчання** Знати принципи і елементи захисту інформації у Microsoft Excel.	4
Тема 5. Захист від несанкціонованого копіювання ***Список рекомендованих джерел:*** *Основний: 2, 3, 4* *Додатковий: 18* Лабораторне заняття № 5 **Пошук паролів у документах Microsoft Office допомогою спеціальних програм** **Мета:** Засвоїти принципи і технологію роботи з програмами дешифраторами паролів Advanced Office Password Recovery. **Завдання:** Ознайомитися з поняттями, принципами роботи та призначення головного меню програм дешифраторів паролів. *1.* Створити файли у Microsoft Word, Excel та встановити паролі, які містять 4 латинських символів. *2.* Знайти вказані паролі за допомогою програми Advanced Office Password Recovery. *3.* Створити файли в Microsoft Word, Excel та встановити паролі, які містять 10 латинських символів та спеціальні символи. *4.* Знайти вказані паролі за допомогою програми Advanced Office Password Recovery. **Результати навчання**	4

1	2
Знати принципи і технології програм дешифраторів паролів.	
Тема 6. Загальні принципи захисту програм від несанкціонованого дослідження ***Список рекомендованих джерел:*** *Основний*: 3, 4, 5. *Додатковий*: 10, 13, 20. Лабораторне заняття № 6 **Шифрування даних за допомогою архіваторів та пошук паролів** **Мета:** засвоїти принципи і технологію роботи з шифрованими архівами та програмами дешифраторів паролів **Завдання:** Ознайомитися із поняттям, принципом роботи та призначенням головного меню програм дешифраторів паролів Ultra Zip Password Cracker та Advanced ZIP Password Recovery. 1. Створити в редакторі Microsoft Word файл довільного змісту. 2. Провести процес архівації без застосування паролів та з їх застосуванням. 3. Спробувати відкрити архіви програмами із пакета Microsoft Office без процесу розархівації. 4. Спробувати відкрити архіви програмами із пакета Microsoft Office після процесу розархівації. 5. Створити архіви .RAR, .ZIP за допомогою програми WinRar та встановити паролі, які містять послідовно: 5,10,15 латинських символів 6. Знайти вказані паролі за допомогою програми Advanced ZIP Password Recovery..	4
Тема 7. Захист від дизасемблювання ***Список рекомендованих джерел:*** *Основний:* 3, 5. *Додатковий:* 16, 18. *Нормативний:* 25, 27 Лабораторне заняття № 7 **Шифрування даних за допомогою спеціальних програм та утиліт** **Мета:** Засвоїти принципи, технологію роботи шифрування та дешифрування файлів. **Завдання:** Ознайомитися із теоретичним відомостями програми Super File Encryption, BestCrypt. 1. Проведіть шифрування двох довільних файлів з диску вашого комп'ютер програмою Super File Encryption. 2. Проведіть дешифрування двох довільних файлів з диску вашого комп'ютер програмою Super File Encryption. 3. Створіть на диску вашого комп'ютера довільний контейнер програмою BestCrypt.	4
Тема 8. Захист від несанкціонованого налагодження ***Список рекомендованих джерел:*** *Основний:* 3, 5. *Додатковий:* 12, 15, 20. Лабораторне заняття № 8 **Захист інформації при застосуванні особистої системи мережевого захисту McAfee Personal Firewall Plus** **Мета:** засвоїти принципи та елементи технології захисту інформації при використанні особистої системи мережевого захисту McAfee Personal Firewall Plus.	8

1	2
Завдання: Навчитися встановлювати програму захисту, проводити конфігурування системи, вводити, видаляти, корегувати Ip адреси постійного та тимчасового доступу, проводити контроль за діями як із середини мережі так і зі сторони Інтернету. Установіть програму на свій комп'ютер, виконавши вказівки п. 1.3. 2. Проведіть запуск програми та уважно вивчіть головне меню програми й зміст вкладок. 3. Проведіть конфігурування програми за допомогою помічника установки. 4. За допомогою вікна Utilities встановіть за чергою різні рівні захисту (табл. 1). 5. Установіть на комп'ютері декілька груп користувачів та надайте їм різні права доступу. 6. Установіть візуальний режим відображення інформації. 7. Установіть на комп'ютері почергово різні типи тривог. 8. Установіть різні параметри в полі Smart Recommendations. 9. Уведіть довільні адреси в список довірених, та таких яким ви тимчасово довіряєте. 11. Проведіть моніторинг трафіку та його аналіз. 12. Закрийте відкриті порти. 13. Опрацюйте звіти. Запишіть головні події у зошит та проведіть їх аналіз. 14. Установіть за чергою різні типи дозволів. 15. Перегляньте файл Подій Реєстрації. 16. Установіть різні типи тривог.	
Тема 9. Криптографічні методи захисту від шкідливих програм ***Список рекомендованих джерел:*** *Основний:* 1, 5. *Додатковий:* 16, 24. *Нормативний:* 25, 27. **Лабораторне заняття № 9** **Шифрування даних** **Мета:** Отримати теоретичні та практичні навички роботи з програмними засобами шифрування даних **Завдання:** 1.Ознайомитися із програмою PGP. Провести операції шифрування і дешифрування над довільними файлами 2. Ознайомитися із програмою TrueCrypt. Створити криптоконтейнер, примонтувати його як віртуальний диск. Помістити в криптоконтейнер довільну інформацію. Відмонтувати диск і перемістити криптоконтейнер. 3. Ознайомитися із програмою LUKS (Linux Unified Key Setup)	4
Тема 11. Особливості зламу автоматизованих систем та програмного забезпечення ***Список рекомендованих джерел:*** *Основний: 1, 3, 5.* *Додатковий: 12, 14, 24.* Лабораторне заняття № 10 **Внутрішній мережевий захист із застосуванням програми LANguard Network Scanner.** **Мета:** засвоїти принципи та елементи технології захисту інформації при використанні програми LANguard Network Scanner. **Завдання:**	8

1	2
1. Запустіть програму LANguard Network Scanner на виконання та познайомтеся з командами головного меню. 2. Налагодьте параметри програми для сканування внутрішньої мережі. 3. Проведіть сканування внутрішньої мережі. 4. Проведіть аналіз результатів сканування для даних, які можуть бути критичними (у протоколі до лабораторної роботи скласти таблицю з коментаріями). 5. Проведіть аналіз результатів сканування для даних, які можуть бути некритичними (у протоколі до лабораторної роботи скласти таблицю з коментаріями) 6. Проведіть повторне налагодження параметрів програми для сканування внутрішньої мережі (параметри повинні відрізнятися від попереднього налагодження). 7. Проведіть повторне сканування внутрішньої мережі. 8. Проведіть порівняння результатів сканування за перший та другий рази. 9. В протоколі для лабораторних робіт складіть табличку з даними, які відрізняються при первинному та повторному скануваннях. Поясніть, чому є відмінності в результатах сканувань. 10. Проведіть роботу з утилітами програми згідно п. 6 теорії. 11. Використайте в роботі команди контекстного меню програми. 12. Результати сканування мережі зберегти на сервері у своєму каталозі. 13. Зробити висновок про захищеність мережі зсередини.	

** всі лабораторні завдання виконуються на основі інтерактивних методів навчання у комп'ютерному середовищі*

САМОСТІЙНА РОБОТА:

Навчальна діяльність	**Робочий час студента (год.)**

1	2
Тема 1. Ведення в надійність та безпеку програмного забезпечення ***Список рекомендованих джерел:*** *Основний: 1* *Додатковий: 7, 8, 10.* *Internet-ресурси: 30* **Самостійна робота:** Проаналізувати найбільш відомі кібератаки за останні роки.	9
Тема 2. Загрози надійності та безпеки програмного забезпечення ***Список рекомендованих джерел:*** *Основний: 1* *Додатковий: 9, 10, 11, 12* *Internet-ресурси: 30* **Самостійна робота:** Проаналізувати можливі наслідки порушення безпеки організацій	9
Тема 3. Загальний огляд систем захисту програмного забезпечення ***Список рекомендованих джерел:*** *Основний: 3* **Самостійна робота:** Проаналізувати сучасні програмні продукти для захисту	9

1	2
програмного забезпечення	
Тема 4. Сучасний стан засобів подолання систем захисту ***Список рекомендованих джерел:*** *Internet-ресурси: 34* **Самостійна робота:** Навести 10 безкоштовних інструментів для моніторингу файлів та папок за змінами у реальному режимі часу.	9
Тема 5. Захист від несанкціонованого копіювання ***Список рекомендованих джерел:*** *Основний: 3* **Самостійна робота:** Розглянути та охарактеризувати наступні ключі захистів: HASP, Hardlock, Sentinel, Guardant.	9
Тема 6. Загальні принципи захисту програм від несанкціонованого дослідження ***Список рекомендованих джерел:*** *Основний: 4* **Самостійна робота**: Навести та описати інструменти, що використовуються зламниками для несанкціонованого дослідження захищених програм.	9
Тема 7. Захист від дизасемблювання ***Список рекомендованих джерел:*** *Основний: 4* **Самостійна робота:** Проаналізувати емуляцію процесора та мультизадачності як засоби протистояння статичному вивченню програм	9
Тема 8. Захист від несанкціонованого налагодження ***Список рекомендованих джерел:*** *Internet-ресурси: 35* **Самостійна робота:** Проаналізувати налагоджувачі: DBG, DDD, DEBUG, Eclipse, GNU Debugger, OllyDbg, Valgrind, Xdebug	7
Тема 9. Криптографічні методи захисту від шкідливих програм ***Список рекомендованих джерел:*** *Основний:* 4. **Самостійна робота:** Проаналізувати спеціалізовані програми, які зашифровують та захищають паролем файли і папки: TrueCrypt, PGP Desktop, R-Crypto, Crypt4Free, RCF EnCoder/DeCoder.	11
Тема 10. Технологія захисту від шкідливих програм ***Список рекомендованих джерел:*** *Основний*: 4. **Самостійна робота:** Проаналізувати існуючі антивірусні програми. Навести їх позитивні та негативні сторони.	6
Тема 11. Особливості зламу автоматизованих систем та програмного забезпечення ***Список рекомендованих джерел:*** *Додатковий:* 24. **Самостійна робота:** Проаналізувати використання хуків у Windows.	12
Тема 12. Захист інформації у комп'ютерних мережах ***Список рекомендованих джерел:*** *Додатковий:* 24. **Самостійна робота:** Проаналізувати сучасні технології дампінга та захист від нього.	9

7. Список рекомендованих джерел

Основний

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. Крепич С.Я., Співак І.Я. Якість програмного забезпечення та тестування. Навчальний посібник. – Тернопіль: ФОП Паляниця В.А., 2020. – 478с.

Додатковий

3. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
4. Гнатовська Г.А. Технологія створення програмних продуктів: конспект лекцій. – Одеса: Одеський державний екологічний університет, 2015. – 97 с.
5. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби : посібник / В.Л. Бурячок, С.В. Толюпа, В.В. Семко та ін. – К. : ДУТ – КНУ, 2016. – 178 с.

Нормативний

6. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. - К.: Держстандарт України, 1998.
7. Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.
8. Закон України «Про захист інформації в інформаційно- телекомунікаційних систе-мах». – К.: Відомості Верховної Ради України, 1994. - N 31. - Ст. 286.
9. Закон України «Про інформацію». – К.:Відомості Верховної Ради України, 1992. - N 48. - Ст.650 .
10. Закон України «Про електронний цифровий підпис». – К.:Відомості Верховної Ради України, 2003. - N 36. - Ст.276 .

Internet-ресурси

11. Програмне забезпечення та його класифікація: - URL: https://kppk.com.ua/ELLIB/ebook/Gorbenko/IKT/3/3.htm
12. Верховна Рада України. Законодавство України: – URL: http://zakon.rada.gov.ua/laws/
13. Державна служба спеціального зв'язку та захисту інформації: – URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/index
14. CERT-UA: – URL: http://cert.gov.ua/
15. 10 Free Tools to Monitor Files and Folders for Changes in Real Time: - https://www.raymond.cc/blog/3-portable-tools-monitor-files-folders-changes/.
16. Налагоджувач: https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D0%BB%D0%B0%D0%B3%D0%BE%D0%B4%D0%B6%D1%83%D0%B2%D0%B0%D1%87.

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*

8. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019 р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/NzU4MQ==/69da3a261374f213990591e6e9a812cd.pdf)

Під час вивчення дисципліни викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється з використанням 365 Office);
- захист лабораторних робіт (проходить під час кожної лабораторної роботи);

- перевірка ходу виконання індивідуального завдання (фінальний проект);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції та заслуховування доповідей на обрані студентами теми;
- перевірка знань отриманих у ході неформальної освіти (додаткові рекомендовані курси).

Розподіл балів за видами діяльності

Вид діяльності	бали
ЛР 1 Захист операційної системи WINDOWS 10.	7
ЛР 2 Захист від фішингових схем в Microsoft Office	6
ЛР 3 Захист інформації у Microsoft Word	6
ЛР 4 Захист інформації в Microsoft Excel	6
ЛР 5 Пошук паролів у документах Microsoft Office допомогою спеціальних програм	6
ЛР 6 Шифрування даних за допомогою архіваторів та пошук паролів	6
ЛР 7 Шифрування даних за допомогою спеціальних програм та утиліт	7
ЛР 8 McAfee Personal Firewall Plus	10
ЛР 9 Шифрування даних	6
ЛР 10 LANguard Network Scanner.	10
Додаткові курси («Introduction to Cybersecurity» академія Cisco)	5
Додаткові бали за відвідування	5
Тест 1	10
Тест 2	10
Разом:	100

9. Політика навчальної дисципліни:

9.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

9.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

9.3. Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)

9.4. За порушення академічної доброчесності студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти КНТЕУ (Наказ КНТЕУ від 02.02.2018 №377. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MTEyNDI=/f78c64a74cbbe5b4238729782d707efa.pdf)