ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ЗАТВЕРДЖУЮ
Голова Вченої ради
Навчально-наукового інституту
цивільного захисту

_____ Василь ПОПОВИЧ
"_04_" _____*вересня*_____ 20*20*р.

ОК 2.12 ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

ПРОГРАМА
навчальної нормативної дисципліни

підготовки бакалавра
спеціальності: 122 Комп'ютерні науки
за освітньою програмою: Комп'ютерні науки

Львів
2020 рік

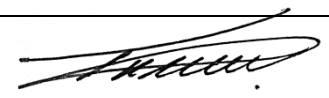
Розробник програми:
Наталія Кухарська, доцент кафедри управління інформаційною безпекою, к. фіз.-мат. наук, доцент

Рецензент: *Наталія Шаховська, завідувач кафедри систем штучного інтелекту Інституту комп'ютерних наук та інформаційних технологій Національного університету «Львівська політехніка», професор, д-р. тех. наук*

Програму рекомендовано кафедрою *управління інформаційною безпекою*

Протокол від "28" *серпня* 2020 року № *1*

Начальник (завідувач) кафедри *управління інформаційною безпекою, доцент, д-р. тех. наук*



_____ *Ростислав ТКАЧУК*
(підпис) (ім'я та прізвище)

Схвалено Вченою радою навчально-наукового інституту *цивільного захисту*

Протокол від "*04*" *вересня* 2020 року № *1*

ВСТУП

Програма вивчення нормативної навчальної дисципліни “Технології захисту інформації” складена відповідно до освітньо-професійної програми підготовки бакалаврів зі спеціальності 122 Комп’ютерні науки.

Предметом вивчення навчального курсу є основні аспекти захисту інформації задля забезпечення безпеки комп’ютерних мереж та інформаційних систем в умовах неповноти та невизначеності вихідних даних. Курсанти та студентив рамках курсу набувають знань в області безпеки комп’ютерних мереж та операційних систем. Дисципліна присвячена вивченню сучасних технологій, які використовуються для організації захисту інформації.

Міждисциплінарні зв’язки. Курс є базовим в програмі підготовки бакалавра за спеціальністю 122 Комп’ютерні науки та має міждисциплінарні зв’язки з такими дисциплінами як: «Комп'ютерні мережі», «Клієнт-серверне програмування», «Операційні системи та системне програмування» та «Комплексні системи санкціонованого доступу».

Програма навчальної дисципліни складається з таких змістовних модулів та тем:

Змістовий модуль 1. Технології захисту інформації

Тема 1. *Вступ. Концепція захисту інформації.*

Тема 2. *Забезпечення безпеки мережевих пристроїв.*

Тема 3. *Авторизація, аутентифікація та акаунтінг.*

Тема 4. *Технології міжмережевого екрану.*

Тема 5. *Системи виявлення та запобігання атак (вторгнень)*

Тема 6. *Забезпечення безпеки локальних мереж*

Змістовний модуль 2. Засоби тестування вразливостей інформаційних систем

Тема 7. *Сканери портів.*

Тема 8. *Сканери вразливостей.*

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. Метою вивчення дисципліни «Технології захисту інформації» формування у здобувачів вищої освіти фахових компетенцій щодо моніторингу, виявлення, аналізу і нейтралізації загроз інформаційної безпеки.

1.2. Основними завданнями вивчення дисципліни “Технології захисту інформації” є:

- засвоєння основних теоретичних, методичних і організаційних основ концептуальних засад забезпечення інформаційної безпеки;
- засвоєння практичних навиків застосування сучасних технологій захисту інформації в комп’ютерних мережах та інформаційних системах;

- засвоєння основних засад щодо використання технологій тестування інформаційних систем на вразливість.

1.3. Програмні результати навчання:

- розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

На вивчення навчальної дисципліни відводиться *90* годин(и)/ *3,0* кредити ECTS.

2. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВИЙ МОДУЛЬ 1.
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Тема 1. ***Вступ. Концепція захисту інформації.***

Сучасні мережеві загрози. Огляд інструментів хакерів. Огляд шкідливого ПЗ (Віруси, трояни, експлоїти тощо). Нейтралізація загроз. Вивчення мережевих атак та інструментів аудиту безпеки.

Тема 2. ***Забезпечення безпеки мережевих пристроїв.***

Захист доступу до пристроїв. Призначення адміністративних ролей. Моніторинг та керування пристроями. Використання автоматичних функції для забезпечення безпеки пристроїв. Захист площини керування. Налаштування Telnet, SSH, Syslog.

Тема 3. ***Авторизація, аутентифікація та акаунтінг.***

Введення у поняття AAA, призначення AAA, локальний AAA, серверний AAA. Налаштування AAA локально. Налаштування віддаленого AAA.

Тема 4. ***Технології міжмережевого екрану***.

Налаштування списків контролю доступу, технології міжмережевих екранів, зональні мережеві екрани. Написання списків контролю доступ. Написання списків контролю доступу зональних міжмережевих екранів.

Тема 5. ***Системи виявлення та запобігання атак (вторгнень)***

Технології IPS та IDS, сигнатури IPS та IDS, впровадження IPS та IDS. Тестування. Реалізація та обговорення завдань. Конфігурування IPS та IDS

Тема 6. ***Забезпечення безпеки локальних мереж***

Безпека кінцевих пристроїв, приклади небезпек 2-го рівня. Реалізація та обговорення завдань. Конфігурування віртуальних локальних мереж то їх захист.

Змістовний модуль 2. Засоби тестування вразливостей інформаційних систем

Тема 7. ***Сканери портів***.

Технології сканування портів. Приклади сканерів портів. Nmap. NetScanTools. SuperScan. IPEYE. FSCAN. WUPS. UDP_SCAN.

Тема 8. ***Сканери вразливостей.***

Можливості сканерів вразливостей Whisker, Nikto, Stealth.

3. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. **Гайворонський М.В**., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009. – 607 с.
2. **Цирлов В.Л.** Основи інформаційної безпеки автоматизованих систем. Короткий курс. Фенікс, 2008. – 173 с.
3. **Домарев В.В.** Безпека інформаційних технологій: Системний підхід. 2008. - 614 с.
4. **ДСТУ 3396.2-97.** Захист інформації. Технічний захист інформації. Терміни та визначення.
5. **Щеглов А.Ю.** Захист комп'ютерної інформації від несанкціонованого доступу. Наука і техніка, Санкт-Петербург. 2004. – 384 с.
6. **Шаньгин В.Ф.** Інформаційна безпека комп'ютерних систем і мереж. Навчальний посібник. Москва: «Форум», 2008. – 416 с.
7. **Лужецький В.А.,** Войтович О.П., Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.
8. **Лужецький В.А.,** Войтович О.П., Дудатьєв А.В. Захист персональних даних. Навчальний посібник. – Вінниця: УНІВЕРСУМ, 2009. – 240 с.

Допоміжна

1. **Кухарська Н. П.** Розробка політики інформаційної безпеки комп’ютерного контролю знань // Вісник ЛДУ БЖД. – 2017. – № 16. – С. 34-39.
2. **Кухарська Н. П**. Програмна реалізація алгоритмів приховування інформації методами довільного інтервалу // Вісник ЛДУ БЖД. – 2018. – № 18. – С. 41-48.
3. **Кухарська Н.П.,** Кордонова Ю.С., Хомич І.В. Використання криптостеганографічного підходу для розв’язування задач захисту інформації // Вісник ЛДУ БЖД. – 2019. – № 20.
4. **Кухарська Н**., Полотай О. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організацій / Кухарська Н., Полотай О. // Інформаційні технології та безпека. Київ, 2019. Т. 7, № 2. С. 126-136.
5. **Соколов А**., Степанюк О. Захист від комп'ютерного тероризму. Довідковий посібник. БХВ-Петербург, Арліт. 2002. – 496 с.
6. **Конеев И.Р**., Беляев А.В. Інформаційна безпека підприємства. – СПб.: БХВ-Петербург, 2003. – 752с.
7. **Чирилло Дж**. Виявлення хакерських атак. Для професіоналів. – СПб.: Питер, 2002. – 864с.
8. **Трофімов В.В**., Ільіна О.П., Кияев В.И., Трофімова Е.В. Інформаційні технології. Під ред. В.В. Трофімова. Підручник. Москва: Юрайт, 2011. – 624 с.
9. **Скиба В.Ю**., Курбатов В.А. Керівництво по захисту від внутрішніх загроз інформаційної безпеки. – СПб.: Питер, 2008. – 320 с.

Інформаційні ресурси

1. **Cyber Security Training. SANS Institute.** Онлайн курси із захисту інформації. [Електронний ресурс]. – Доступний з http://www.sans.org
2. Інформаційний онлайн-журнал **Infosecurity** [Електронний ресурс]. – Доступний з https://www.infosecurity-magazine.com/

4. КРИТЕРІЇ УСПІШНОСТІ НАВЧАННЯ ТА ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ

При оцінюванні результатів навчання здобувачів освіти потрібно керуватися такими **критеріями успішності навчання**:

Бали	Оцінка	Критерії оцінювання
91–100	**Відмінно**	Здобувач демонструє повні й вичерпні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни при розв'язуванні практичних завдань, може аналізувати і співставляти навчальний матеріал з даної та суміжних дисциплін. Знає сучасні технології та методи рішення прикладних завдань з дисципліни. За час навчання при проведенні лабораторних занять, виконанні індивідуальних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни яка вивчається, але виходить за рамки об'єму матеріалу передбаченого робочою програмою, або здобувач проявляє невпевненість в тлумаченні теоретичних положень чи рішенні складних практичних завдань.
81–90	**Добре**	Здобувач демонструє добрі та вичерпні знання, володіє матеріалом, що відповідає робочій програмі дисципліни, робить на основі здобутих знань аналіз можливих ситуацій та вміє застосовувати теоретичні положення при рішенні практичних завдань, проте допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи рішення практичних завдань з дисципліни. За час навчання при проведенні лабораторних занять, виконанні індивідуальних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.
71–80	**Добре**	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для рішення характерних/типових прикладних

		завдань з дисципліни. Вміє пояснити основні положення виконаних завдань та давати правильні відповіді про зміну результату при заданій зміні вихідних параметрів. Помилки у відповідях / рішеннях / розрахунках не є системними. Розуміє основні положення, що мають визначальне значення для лабораторних занять, виконанні індивідуальних завдань в межах дисципліни.
61–70	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати завдання подібні тим, що розглядались на заняттях, проте допускає значну кількість неточностей і помилок, усунути які здатен лише за допомогою викладача.
51–60	**Задовільно**	Здобувач володіє певними знаннями та основними положеннями, передбаченими робочою програмою дисципліни, на мінімально допустимому рівні для подальшого засвоєння результатів навчання в рамках освітньої програми. З використанням основних теоретичних положень здобувач з труднощами пояснює правила вирішення практичних завдань дисципліни. Виконання лабораторних, індивідуальних завдань, значно формалізовано: є відповідність алгоритму, проте відсутнє глибоке розуміння самої роботи.
35–50	**Незадовільно**	Здобувач може відтворити окремі фрагменти знань з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час лабораторних занять та результати поточного контролю в більшості є невірними та/або необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні, що створює перепони для подальшого засвоєння результатів навчання в рамках освітньої програми.
0–34	**Незадовільно**	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його відповіді під час лабораторних занять та результати поточного контролю є невірними та/або необґрунтованими. Його знання на підсумкових етапах навчання є фрагментарними.

Формою підсумкового контролю є диференційований залік.

5. ЗАСОБИ ДІАГНОСТИКИ УСПІШНОСТІ НАВЧАННЯ

Під час вивчення дисципліни передбачено індивідуальний поточний контроль, фронтальний контроль, контроль за виконанням самостійної роботи, самоконтроль та індивідуальний підсумковий контроль у формі диференційованого заліку. Поточний контроль здійснюється у формі виконання тестових завдань на базі платформи віртуального навчального середовища. Самоконтроль організовано шляхом надання здобувачам освіти другої спроби

для складання тестових завдань (можливість надолуження пройденого матеріалу та перевірки рівня його засвоєння). Фронтальний контроль передбачає проведення наскрізного тестування або усного опитування під час лекційних занять з метою визначення якості засвоєння нового матеріалу. Під час лабораторних занять або/та консультацій викладач здійснює контроль за самостійною роботою здобувачів освіти шляхом захисту звітів лабораторних робіт. Індивідуальний підсумковий контроль здійснюється у формі диференційованого заліку.

Усі форми контролю включено до 100-бальної шкали оцінювання. Оцінка із 100-бальної шкали в національну переводиться відповідно до діючого положення про освітній процес (91–100 – «відмінно», 71–90 – «добре», 51–70 – «задовільно», менше 51 – «незадовільно»).