ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ЗАТВЕРДЖУЮ
Голова Вченої ради
Навчально-наукового інституту
цивільного захисту

_____ Василь ПОПОВИЧ
"_04_" _____вересня_____ 2020р.

ОК 2.25 КОМПЛЕКСНІ СИСТЕМИ САНКЦІОНОВАНОГО ДОСТУПУ

ПРОГРАМА
навчальної нормативної дисципліни

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

Львів
2020 рік

Розробники програми:
Андрій Лагун, доцент кафедри управління інформаційною безпекою, доцент, канд. тех. наук
Володимир Самотий, професорк кафедри управління інформаційною безпекою, доцент, д-р. тех. наук

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* 20*20* року № *1*

Начальник (завідувач) кафедри *управління інформаційною безпекою*

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

Схвалено Вченою радою навчально-наукового інституту *цивільного захисту*

Протокол від "*04*" *вересня* 20*20* року № *1*

ВСТУП

Програма вивчення нормативної навчальної дисципліни “Комплексні системи санкціонованого доступу” складена відповідно до освітньо-професійної програми підготовки бакалаврів зі спеціальності 122 “Комп’ютерні науки”.

Предметом вивчення навчального курсу є системи санкціонованого доступу до інформації та об’єкти критичної інформаструктури.

Міждисциплінарні зв’язки. Курс є нормативним в програмі підготовки бакалавра за спеціальністю 122 “Комп’ютерні науки” та має міждисциплінарні зв’язки з навчальною дисципліною «Технології захисту інформації».

Програма навчальної дисципліни складається з такого **змістовного модуля та тем**:

Змістовий модуль 1. Підходи та принципи забезпечення санкціонованого доступу

Тема 1. Законодавча, наукова та нормативно-методологічна база.

Тема 2. Основи побудови комплексної системи санкціонованого доступу.

Тема 3. Аналіз можливих загроз безпеці інформації.

Тема 4. Автоматизовані системи управління доступом.

Тема 5. Методи та засоби ідентифікації осіб.

Тема 6. Реалізація систем контролю доступу.

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. Метою навчальної дисципліни “Комплексні системи санкціонованого доступу” є формування у здобувачів освіти системи теоретичних, методичних та наукових знань щодо організації комплексної системи захисту інформації, аспектами її практичного застосування та розробки, забезпечення функціонування та контролю за її ефективністю.

1.2. Основними завданнями вивчення дисципліни «Комплексні системи санкціонованого доступу» є:

- засвоєння основних теоретичних, методичних і організаційних основ концептуальних засад забезпечення інформаційної безпеки;
- ознайомлення з основними поняттями та категоріями інформаційна безпека, як складової національної безпеки;
- оволодіння знаннями з основних принципів та етапі розробки системи захисту інформації;
- формування комплексного бачення умови розробки, проектування, випробування та експлуатації комплексної системи захисту інформації.

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

● шляхом організаційних, програмних та технічних засобів забезпечувати санкціонований доступ на підприємства чи організації будь якої форми власності на основі існуючих технологій ідентифікації осіб (механічний, магнітний, оптичний, біометричний, комбінований).

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

2. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВИЙ МОДУЛЬ 1.
ПІДХОДИ ТА ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ САНКЦІОНОВАНОГО ДОСТУПУ.

Тема 1. Законодавча, наукова та нормативно-методологічна база

Основні законодавчі акти та нормативні документи, що регламентують діяльність у сфері ЗІ. Введення нових законів,ДСТУ, положень, постанов та інструкцій, які регулюють юридичну відповідальність посадових осіб, користувачів та обслуговуючого технічного персоналу за витік, втрату або модифікацію довіреної йому інформації, яка підлягає захисту.

Тема 2. Основи побудови комплексної системи санкціонованого доступу

Основні терміни та визначення. Вимоги до системи безпеки на підприємстві та основні принципи її побудови. Етапи створення комплексної системи санкціонованого доступу.

Тема 3. Аналіз можливих загроз безпеці інформації

Загальні положення. Аналіз можливих збитків від дій зловмисників. Можливі джерела загроз.

Тема 4. Автоматизовані системи управління доступом

Загальні положення. Основні компоненти АСУД. Вимоги до функціональних характеристик АСУД.

Тема 5. Методи та засоби ідентифікації осіб

Загальні положення ідентифікації осіб. Ідентифікація за допомогою механічних ключів та перепусток. Парольна ідентифікація. Апаратна ідентифікація. Біометрична ідентифікація.

Тема 6. Реалізація систем контролю доступу

Загальна характеристика систем контролю доступу. Автономні системи санкціонованого доступу. Мережеві та універсальні системи контролю доступу. Елементи системи контролю доступу. Елементи обладнання перепони комплексної системи санкціонованого доступу. Організація доступу на об’єкт. Система управління доступом у кілька внутрішніх приміщень однієї будівлі. Організація автоматизованої прохідної. Централізоване управління доступом підприємства. Методика побудови системи санкціонованого доступу на об’єкт. Відеоспостереження як складова частина комплексних систем санкціонованого доступу. Інші аспекти побудови комплексної системи санкціонованого доступу.

3. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. **Гарасимчук О. І.** Комплексні системи санкціонованого доступу : навч. посібник / О. І. Гарасимчук, В. Б. Дудикевич, В. А. Ромака ; Львів. політех. - Л. : Вид-во Львів. політехніки, 2010. - 212 с.
2. **Девянин П.Н.** Моделі безпеки комп'ютерних систем: Навчальний посібник. – М.: «Академія», 2005. – 114 с.
3. **Домарєв В.В., Скворцов С.О.** Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.
4. **Домарєв В.В., Швець В.А., Шестакова В.В.** Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
5. **Дудатьєв А.В.** Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-Сум-Вінниця, 2009. – 240 с.
6. **Завгородний В.І.** Комплексний захист інформації в комп'ютерних системах – М.: Логос; 2001. – 264 с.
7. **Качинський А.Б.** Безпека, загрози і ризик: наукові концепції та математичні методи / Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К.: 2004. – 472 с.
8. **Юдін О.К., Корченко О.Г., Конахович В.Г.** Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

Допоміжна

1. **Лагун А. Е.** Теорія інформації та кодування : навч. посібн. / А. Е. Лагун, Ю. І. Грицюк. – Львів : СПОЛОМ, 2016. – 168 с.
2. **Kukharska N., Lagun A., Polotai O.** The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020 (Lviv, august 21–25, 2020). Lviv, 2020. Pp. 538–541
3. **Lagun A.** Embedding of the hidden information with the use of Discrete Fourier Transform [Electronic resource] / A. Lagun, N. Kukharska // Automatic Control and Information Technology (ICACIT’17) : 4th International Conference, 14-16 December 2017 : Proceedings. – Cracow, 2017. – 1 electr. opt. disk (CD-ROM).
4. **Совин Я. Р.** Мікропроцесори в системах технічного захисту інформації.: навчальний посібник / Я. Р. Совин, Ю. М. Наконечний. – Львів: Видавництво Львівської політехніки, 2011. – 308 с. Рекомендовано МОН України.
5. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009. – 607 с.

6. **Домарев В.В.** Безпека інформаційних технологій: Системний підхід. 2008. - 614 с.

7. **ДСТУ 3396.2-97.** Захист інформації. Технічний захист інформації. Терміни та визначення.

8. Закон України «Про захист інформації в інформаційно телекомунікаційних системах», від 05.07.1994 № 80/94-ВР (Зі змінами, внесеними згідно із Законом № 1703-IV від 11.05.2004, в редакції Закону № 2594-1V від 31.05.2005, ВВР, 2005, № 26, ст. 347).

9. **Лужецький В.А., Войтович О.П., Дудатьєв А.В.** Захист персональних даних. Навчальний посібник. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.

10. **Скиба В.Ю., Курбатов В.А.** Керівництво по захисту від внутрішніх загроз інформаційної безпеки. – СПб.: Питер, 2008. – 320 с.

11. **Цирлов В.Л.** Основи інформаційної безпеки автоматизованих систем. Короткий курс. Фенікс, 2008. – 173 с.

12. **Шаньгин В.Ф.** Інформаційна безпека комп'ютерних систем і мереж. Навчальний посібник. Москва: «Форум», 2008. – 416 с.

13. **Щеглов А.Ю.** Захист комп'ютерної інформації від несанкціонованого доступу. Наука і техніка, Санкт-Петербург. 2004. – 384 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 практичних 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 практичних 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 практичних 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 практичних, 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 практичних 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 практичних 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, індивідуальний підсумковий контроль у формі диференційованого заліку. Поточний контроль здійснюється у формі усного та письмового опитування та виконання практичних робіт. Фронтальний контроль передбачає проведення наскрізного тестування або усного опитування під час лекційних занять з метою визначення якості засвоєння нового матеріалу. Індивідуальний підсумковий контроль здійснюється у формі 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»).