СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Програмні методи захисту інформації»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	магістр
	Галузі знань ……	12 Інформаційні технології 17 Електроніка, автоматизація та електронні комунікації
	Тривалість викладання	3,4 чверті
	Заняття:	весняний семестр
	лекції:	2 години
	практичні заняття:	1 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=5227

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів

Сафаров Олександр Олександрович	к.т.н.
Персональна сторінка	**https://bit.nmu.org.ua/ua/pro_kaf/prepods/saforov.php**
E-mail:	safarov.o.o@nmu.one

Анотація до курсу

Програмні методи захисту інформації - це дисципліна для вивчення системних та прикладних методів, які призначені для захисту інформації, що передається по телекомунікаційним каналам. Найчастіше програмні засоби захисту інформації застосовують для виконання таких процесів як ідентифікація й автентифікація користувачів, розмежування доступу користувачів до інформаційної мережі, парольний захист і перевірка повноважень, шифрування інформації, а також її захист від несанкціонованих змін, зчитування, копіювання.

1. Мета та завдання курсу

Мета дисципліни – закласти термінологічний фундамент, навчити здобувачів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам та засобам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу:
У результаті вивчення курсу студенти повинні вивчити: методи забезпечення функціонування спеціального програмного забезпечення щодо захисту даних від руйнуючих програмних засобів та проводити аналіз ефективності систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів.

2. Результати навчання:

Отримання знань та навичок у використанні сучасних методів розроблення програмних засобів захисту інформації та синтезу комплексів засобів захисту інформації.

У результаті навчання студенти навчаться наступному:

Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, систем виявлення та запобігання атакам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури, зокрема із використанням імітаційних моделей процесів.

Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи та моделі кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

4. Структура курсу.

ЛЕКЦІЇ **80**

Тема 1. Базові поняття інформаційної безпеки
Основні поняття. Захист інформації та його основні завдання. Класифікація загроз для інформації та їх джерел. Поняття про інформацію з обмеженим доступом. Структура політики безпеки та її основні частини.

Тема 2. Механізми і політики розмежування прав доступу
TCSEC - перший стандарт у галузі оцінки захищеності комп'ютерних систем. Common Criteria - європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Вимоги довіри. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу"

Тема 3. Шифрування даних.
Основні поняття роботи К. Шеннона "Теорія зв'язку в секретних системах". Симетричні, асиметричні та комбіновані криптосистеми. Їх переваги та недоліки.

Тема 4. Системи захисту програмного забезпечення.
Мета і доцільність використання систем захисту. Класифікація системи захисту інформації. Пакувальники/шифратори. Системи захисту від несанкціонованого копіювання. Системи захисту від несанкціонованого доступу. Основні алгоритми захисту програмного забезпечення.

Тема 5. Розповсюджені типи захистів та їх недоліки.
Основні вимоги до розробки систем захисту. Розповсюджені типи захистів та їх недоліки
Тема 6. Засоби подолання систем захисту.
Проблема існування засобів зламу захистів програмного забезпечення. Класифікація засобів подолання систем захисту програмного забезпечення. Програми розпакування, дешифрування та криптоаналізу.
Тема 7. Основні поняття ОС, необхідні для створення систем захисту.
Склад операційної системи. BIOS. CMOS. Переривання, їх роль і процедура звертання в програмах. Робота з дисками на фізичному рівні.
Тема 8. Загальні принципи захисту програм від несанкціонованого дослідження.
Принципи побудови систем захисту та їх функції. Основні методи та засоби дослідження програм. Способи вбудовування захисних механізмів в програмне забезпечення. Структура програм, захищених від дослідження.
Тема 9. Захист від дизасемблювання.
Необхідність і доцільність захисту від дизасемблювання. Основні методи протидії дизасемблюванню програм. Поняття обфускації та його види.
Тема 10. Захист від несанкціонованого налагоджування
Огляд і класифікація налагоджувачів. Захист від налагоджувачів реального режиму. Боротьба з налагоджувачами захищеного режиму. Додаткові прийоми антиналагоджувального програмування.

ПРАКТИЧНІ ЗАНЯТТЯ **40**

Практична робота №1
Тема: Розмежування повноважень користувачів на основі парольної аутентифікації.
Мета роботи: Розробка програми розмежування повноважень користувачів на основі парольної аутентифікації.
Завдання: Розробити програму розмежування повноважень користувачів на основі парольної аутентифікації.

Практична робота №2
Тема: Логування дій користувачів у програмних системах.
Мета роботи: Засвоїти методику та отримати практичні навики розробки процедур логування дій користувачів на прикладі підсистем ідентифікації та аутентифікації користувачів із важкооборотними однонапрямленими хеш-функціями.
Завдання: Удосконалити розроблену в лабораторній роботі № 1 програмну систему з метою покращення функції ідентифікації та аутентифікації користувачів.
Практична робота №3
Тема: Методи захисту програмного забезпечення.
Мета роботи: Одержати практичні навики реалізації алгоритмів захисту програмного забезпечення для найпоширеніших моделей розповсюдження.
Завдання: 1. Розробити програмний продукт (або удосконалити ПЗ розроблене в попередніх лабораторних роботах), що виконує мінімум 10

функцій (для прикладу - відкриття файлу, збереження файлу, довідка, друк, перегляд параметрів файлу, пошук та інші).

РАЗОМ **120**

5. Технічне обладнання та/або програмне забезпечення.

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
53	42	30	5	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

53 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

14 балів – Достатня зрозумілість відповіді

10 бали – Добра зрозумілість відповіді

6 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". https://cutt.ly/IBesJEc.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов’язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об’єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни. За участь у анкетуванні здобувач вищої освіти отримує **5 балів**.

8 . Рекомендовані джерела інформації

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
2. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
3. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифровихзасобів негласного отримання інформації. К. Міленіум. 2020. 326 с.
4. Nadalin Alessandro. WASEC: Web Application Security for the everyday software engineer: Everything a web developer should know about application security: concise, condensed and madetolast/ A. Nadalin. — Leanpub, 2020. — 161 p.— ISBN 1670062449, 9781670062444.
5. S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milovandothers. Synergy of building cyber security systems: monograph. Kharkiv: PC TECHNOLOGYCENTER, 2021. 188 p.