СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ПЛАНУВАННЯ ТА ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ»

Ступінь освіти	магістр
Галузь знань	12 Інформаційні технології
Тривалість викладання	1, 2 чверті
Заняття:	І семестр 2024/2025 н.р.
Лекції	1 година на тиждень
Лабораторні	1 година на тиждень
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=6657#section-2

Кафедра, що викладає: Інформаційних технологій та комп'ютерної інженерії

Інформація про викладача:

Викладач:	Каштан В.Ю., доцент.
Персональна сторінка:	https://it.nmu.org.ua/ua/HR_staff/preps/kashtan.php
E-mail:	Kashtan.V.Yu@nmu.one

1. Анотація до курсу

Темпи розвитку інформаційних технологій за останні 20 років сприяли впровадженню засобів обчислювальної техніки у всі сфери людської діяльності. Це у свою чергу, позначилось на попиті інтересу до інформації, що циркулює всередині інформаційних систем, не тільки з боку законних користувачів та власників, а й з боку зловмисників. Тому, проблема інформаційної безпеки має важливе значення з точки зору розробки інформаційних систем.

Головно причиною інтересу до інформаційних систем є помітне спрощення методів та засобів одержання та використання інформації.

Сьогодні існує велика кількість каналів витоку інформації. Це і природні канали, що утворюються з певних фізичних явищ і процесів, і штучні канали витоку інформації, які створюються навмисно із застосуванням активних методів та засобів отримання інформації. Тому, актуальним є розробка методів та засобів захисту інформації від порушення її фізичної та логічної цілісності, а також несанкціонованого доступу. Причому всі ці методи та засоби, як правило, через тісний взаємозв'язок розвиваються паралельно з розвитком самих електронних засобів обробки даних.

Навчальна дисципліна «**Планування та організація захисту інформаційних систем»** знайомить здобувачів вищої освіти з сучасними інформаційних технологіями у галузі інформаційної безпеки та криптографічних методів захисту інформації, тощо. Це дозволить майбутньому фахівцю планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації.

2. Мета та завдання навчальної дисципліни

Мета викладання навчальної дисципліни – підготовка спеціалістів за другим освітньо-кваліфікаційним рівнем магістра відповідно до державних стандартів, встановлених освітньо-кваліфікаційною характеристикою (ОКХ) та освітньо-професійною програмою (ОПП) підготовки магістрів вищезазначеного фахового спрямування.

Мета навчальної дисципліни – формування у здобувачів вищої освіти компетентностей щодо вивчення методологічних, організаційних та наукових основ розробки засобів і систем збору, захисту інформації та застосування методів та засобів захисту інформації в інформаційних системах.

Завдання курсу:

– ознайомити здобувачів вищої освіти з організаційними основами забезпечення інформаційної безпеки України;

– ознайомити здобувачів вищої освіти із основними підходами до управління інформаційною безпекою;

– ознайомити здобувачів вищої освіти з методами та засоби криптографічного та стеганографічного захисту інформації, що циркулює у інформаційних системах;

– вивчення видів загроз інформаційній безпеці та технічних каналів витоку інформації;

– ознайомити здобувачів вищої освіти з методами і заходами протидії кіберінцидентам, надавати рекомендації щодо попередження та аналізу кіберінцидентів.

3. Результати навчання

1. Аналізувати систему управління безпекою, оцінювати її спроможність та достатність для прийняття обґрунтованих рішень у сфері інформаційної безпеки.

2. Вміти здійснювати попередню оцінку можливості застосування нейронної мережі для вирішення поставленої задачі.

3. Використовувати методи захисту інформації в інформаційних системах та давати оцінку якості прийнятих рішень.

4. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів для безпеки інформаційних систем.

5. Здійснювати планування та управляти заходами безпеки професійної діяльності, проявляти ініціативність, автономність та відповідальність при прийнятті рішень.

4. Структура курсу

ЛЕКЦІЇ

1 Концептуальні засади забезпечення інформаційної безпеки України для інформаційних систем

1.1 Нормативно-правові основи захисту інформації в Україні
1.2 Концепція національної безпеки України.
1.3 Концепція інформаційної безпеки України.
1.4 Управління безпекою. Розробка правил безпеки.

2 Загрози безпеки інформаційним системам

2.1 Випадкові загрози.
2.2 Навмисні загрози.
2.3 Класифікація загроз

3 Канали витоку інформації

3.1 Характеристика каналів витоку інформації
3.2 Канали витоку інформації при експлуатації електронних девайсів.

4 Методи захисту інформації в інформаційних системах

4.1 Класифікація методів захисту інформації від випадкових загроз.
4.2 Технічні методи захисту інформації
4.3 Методи захисту інформації від несанкціонованого доступу.

5 Криптографічні методи захисту інформації

5.1 Класифікація криптографічних методів.
5.2 Шифр заміни.
5.3 Шифр перестановки
5.4 Шифр Вернама.
5.5 Шифри з ключами.
5.6 Методи симетричної криптографії.
5.7 Методи асиметричної криптографії.
5.8 Проблеми та перспективи криптографічних систем.

6 Програмні методи захисту інформації в інформаційних системах

6.1 Програмне забезпечення та інформаційна безпека.
6.2 Контроль життєвого циклу програмного забезпечення.
6.3 Методи захисту від шкідливого програмного забезпечення
6.4 Технологія VPN

7 Планування захисту інформації

7.1 Інциденти у сфері високих технологій.

7.2 Політика реагування на кіберінциденти.

7.3 Етапи відновлення стану кібербезпеки.

7.4 Захист інформації в геоінформаційних системах і системах управління базами даних

ЛАБОРАТОРНІ ЗАНЯТТЯ

Лабораторна робота 1	Аналіз відомостей про атаки в інформаційних системах.
Лабораторна робота 2	Аналіз каналів витоку інформації та механізм їх утворення.
Лабораторна робота 3	Дослідження методів створення та збереження надійних паролів.
Лабораторна робота 4	Дослідження криптографічних методів захисту інформації.
Лабораторна робота 5	Дослідження режимів шифрування блокових шифрів.
Лабораторна робота 6	Вивчення процесів, потоків, дескрипторів та реєстру Windows з точки зору безпеки операційної системи.
Лабораторна робота 7	Інтеграція захисту даних в геоінформаційній системі QGIS і СУБД.

5. Технічне обладнання та/або програмне забезпечення

Використовуються лабораторна та інструментальна бази випускової кафедри інформаційних технологій та комп'ютерної інженерії, а також комп'ютерне та мультимедійне обладнання:

1. Персональний комп'ютер або ноутбук зі сталим доступом до мережі Інтернет

2. Активований акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365.

3. Активний обліковий запис у системі дистанційної освіти Moodle.

4. Дистанційна платформа Moodle: https://do.nmu.org.ua/course/view.php?id=3766

5. Програмне забезпечення:

- платформа Windows 10;
- Microsoft Office або LibreOffice;
- інтернет-браузер.

6. Система оцінювання та вимоги

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

Рейтингова	**Інституційна**
90…100	відмінно / Excellent

74…89	добре / Good
60…73	задовільно / Satisfactory
0…59	незадовільно / Fail

6.2. Здобувач вищої освіти може 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.

Поточна успішність складається з оцінок за лекційну частину курсу та лабораторний практикум. Отримані бали додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Максимальне оцінювання:

Теоретична частина	**Лабораторна частина**		**Разом**
	При своєчасному складанні	**При несвоєчасному складанні**	
50	50	40	100

В рамках курсу передбачено виконання 7 лабораторних робіт. Під час захисту лабораторної роботи здобувач відповідає на запитання стосовно ходу роботи, пояснює послідовність дій, демонструє результати роботи.

За результатами виконання лабораторної роботи здобувачі складають звіт встановленого зразка, який завантажується до системи Moodle у відповідну категорію.

Звіт обов’язково має містити такі структурні компоненти:

- титульний лист;

- номер варіанту, текст завдання;

- скріншоти етапів виконання завдання, посилання на відповідні ресурси, коди програм тощо;

- звіт має бути завантажено у систему впродовж 3 днів після захисту роботи на занятті.

Важливо!!! Всі умови до лабораторних робіт з детальними поясненнями до них представлено на сторінці Moodle. Всі бали за лабораторні роботи фіксуються у журналі оцінок Moodle.

6.3. Критерії оцінювання теоретичної частини курс.

Під час проведення контрольних заходів наприкінці третьої та четвертої чверті здобувачі вищої освіти складають відповідні тести, кожен з яких складається з 25

питань. На кожне питання надається 4 варіанти відповіді, серед яких лише 1 – вірний. Максимальна оцінка за тест складає 25 балів, максимальна оцінка за теоретичну частину курсу (сума оцінок за 2 тести) – 50 балів. Опитування за тестом проводиться з використанням системи дистанційної освіти Moodle.

6.4. Критерії оцінювання лабораторної роботи.

З кожної лабораторної роботи здобувач вищої освіти отримує 5 запитань з переліку контрольних запитань. Відповідь на питання оцінюється максимально у 2 бал, причому:

- **2 бали** – відповідь правильна:
- **1 бал** – відповідь вірна, але не повна;
- **0, 5 бали -** ; відповідь вірна, але містить неточності та/або помилки;
- **0 балів** – відповідь неправильна.

Максимальна оцінка за лабораторну роботу складає 10 балів. Максимальна оцінка за лабораторний практикум – 50 балів.

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://www.nmu.org.ua/ua/content/activity/us_documents.pdf .

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. 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.

7.5. Політика щодо оскарження оцінювання

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

7.6. Студентоцентрований підхід

Для врахування інтересів та потреб студентів на початку вивчення курсу здобувачам вищої освіти пропонується відповісти у системі Moodle на низку питань щодо інформаційного наповнення курсу. Відповідно до результатів опитування формується траєкторія навчання з урахуванням потреб студентів.

Під час навчання здобувачі вищої освіти реалізують своє право вибору індивідуальних завдань лабораторних робіт.

Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освітим пропонується анонімно заповнити у системі Moodle або Teams електронні анкети для оцінки рівня задоволеності методами навчання і викладання та врахування пропозицій стосовно покращення змісту навчальної дисципліни. За результатами опитування вносяться відповідні корективи у робочу програму та силабус.

8. Рекомендовані джерела інформації

1. 1. Стандарт вищої освіти України: другий (магістерський) рівень, галузь знань 12 − Інформаційні технології, спеціальність 126 – Інформаційні системи та та технології. Затверджено Наказом Міністерства освіти і науки України 30.12.2021 р. № 1497. – 16 с.

2. Закон України „Про Державну службу спеціального зв'язку та захисту інформації України".

3. Закон України „Про інформацію".

4. Закон України „Про наукову і науково-технічну експертизу".

5. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.

6. Голінько В.І. Управління безпекою в професійній діяльності. Навчальний посібник. – Д.: НТУ «Дніпровська політехніка», 2018. – 157 с

7. Aboul Ella Hassanien, Mohamed Elhoseny. Cybersecurity and Secure Information Systems. – 2019, 156 p.

8. Harold F. Tipton, Micki Krause. Information Security Management Handbook. - 6th ed., 458 p., 2019.