СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Ступінь освіти	бакалавр
Спеціальність	122 Комп'ютерні науки
Освітня програма	Комп'ютерні науки
Тривалість викладання	11, 12 чверть
Заняття:	весняний семестр
лекції:	2 години
лабораторні заняття:	1 година
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:https://do.nmu.org.ua/course/view.php?id=4014

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладача:

Корченко Анна Олександрівна	д.т.н., професор, професор кафедри безпеки інформації та телекомунікацій
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/Korchenko.php
E-mail:	Korchenko.A.O@nmu.one

1. Анотація до курсу

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» входить до складу обов'язкових дисциплін більшості спеціальностей 12 галузі знань «Інформаційні технології». Вона присвячена розгляду стандартів, методів та засобів проектування, впровадження та підтримки захищених інформаційних систем. В курсі розглядаються сучасні підходи до забезпечення захисту інформаційних активів, приділяється певна увага процесам оцінки захищеності систем і технологій обробки інформації. Розглянуті складові комплексних систем захисту інформації. Надані певні відомості про методи протидії актуальним кіберзагрозам.

2. Мета та завдання курсу

Мета дисципліни – формування компетентностей щодо використання сучасних процедур забезпечення безпеки інформації, складових та принципів кіберзахисту.

Завдання курсу:

- ознайомити здобувачів вищої освіти з певними практиками побудови та використання захищених інформаційних систем;
- вивчити особливості реалізації систем захисту у гетерогенному інформаційному середовищі;
- закріпити знання та навички з адміністрування та експлуатації інформаційно-телекомунікаційних систем;
- навчити здобувачів вищої освіти використовувати вітчизняні та міжнародні стандарти і нормативні документи з метою побудови кіберстійких рішень.

3. Дисциплінарні результати навчання

Дисциплінарні результати навчання:

– вміти використовувати стандартні методи аналізу захищеності систем та технологій обробки інформації, створювати моделі загроз, порушника в інформаційних та інформаційно-телекомунікаційних системах;

– вміти використовувати мережні технології в процесі проектування захищеного програмного забезпечення;

– обґрунтовано використовувати процедури вибору захищених рішень в процесі створення і використання інформаційних систем та технологій;

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

4. Структура курсу

Види та тематика навчальних занять	**Внесок в загальну оцінку, %**
ЛЕКЦІЇ	**40**
1. Термінологія безпеки інформації.	
2. Типові вразливості систем і аналіз причин їх появи.	
3. Загрози та порушники безпеки інформації.	
4. Теоретичні основи захисту інформації.	
5. Будова систем захисту інформації.	
Тестова контрольна робота №1 (за темами 1-5).	20
6. Шкідливе програмне забезпечення	
7. Вітчизняні та міжнародні стандарти при побудові кіберстійких рішень.	

Види та тематика навчальних занять	Внесок в загальну оцінку, %
8. Основи криптографічних методів захисту інформації.	
9. Безпека в комп'ютерних мережах.	
Тестова контрольна робота №2 (за темами 6-9).	20
ЛАБОРАТОРНІ ЗАНЯТТЯ	**60**
Лабораторна робота 1 Оцінка ризиків інформаційної безпеки.	
Звіт з роботи № 1 та захист лабораторної роботи.	20
Лабораторна робота 2 Розробка моделей порушника та загроз при роботі в комп'ютерних мережах.	
Звіт з роботи № 2 та захист лабораторної роботи.	20
Лабораторна робота 3 Розробка політики безпеки інформації в інформаційних системах.	
Звіт з роботи № 3 та захист лабораторної роботи.	20
РАЗОМ	**100**

5. Технічне обладнання та/або програмне забезпечення

№ роботи (шифр)	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
Лабораторна робота 1	Оцінка ризиків інформаційної безпеки.	Персональний комп'ютер Платформа MS Windows або Ubuntu MS Office, або MS Office 365 або LibreOffice Калькулятор ризиків FAIR-U Пакет DS Office
Лабораторна робота 2	Розробка моделей порушника та загроз при роботі в комп'ютерних мережах.	Персональний комп'ютер Платформа MS Windows або Ubuntu BoUML, MS Office, або MS Office 365 або LibreOffice
Лабораторна робота 3	Розробка політики безпеки інформації в інформаційних системах.	Персональний комп'ютер Платформа MS Windows або Ubuntu OpenJDK NetBeans або IntelliJ IDEA MS Office, або MS Office 365 або LibreOffice

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 захисту лабораторних робіт складатиме не менше 60 балів.

Теоретична частина оцінюється за результатами здачі двох контрольних тестових робіт, кожна з яких містить тестові закриті запитання з однією вірною відповіддю (максимальна кількість – 20 балів за кожною тестовою роботою). Загалом за дві контрольні тестові робіти отримується максимум 40 балів, тобто 40% від оцінки за дисципліну.

Лабораторні роботи (три роботи – у вигляді індивідуального завдання з кожної, розподіл % див. в таблиці розділу 4) виконуються у письмовому вигляді (звіт з кожної роботи оцінюється в межах балів, представлених в таблиці розділу 4, загалом лабораторні враховуються як 60% (максимум 60 балів). Отримані бали за теоретичну частину та лабораторні роботи додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

6.3. Критерії оцінювання підсумкової роботи. У випадку якщо здобувач вищої освіти за поточною успішністю отримав менше 60 балів та/або прагне поліпшити оцінку, проводиться підсумкове оцінювання.

Підсумкове оцінювання за дисципліною проводиться у вигляді комплексної контрольної роботи, яка включає запитання з теоретичної та практичної частини курсу. Білет складається з 30 тестових завдань з чотирма варіантами відповідей, одна правильна відповідь оцінюється в 2 бали (разом 60 балів) та 2 завдань з практичної частини, кожне з запитань оцінюється максимум у 20 балів (разом 40 балів).

Отримані бали за тестові завдання та завдання з практичної частини додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за підсумковою роботою здобувач вищої освіти може набрати 100 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).

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.

8 Рекомендовані джерела інформації

1. Захист інформації в комп'ютерних системах та мережах: навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків: НТУ "ХПІ", 2014. – 251 с.

3. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсеєв С.П., Король О.Г. – Львів: «Новий світ-2000», 2019. – 678 с.

4. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 2019.
https://er.nau.edu.ua/handle/NAU/39122?mode=full

4. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

6. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту.

Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

8. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)