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

Ступінь освіти	бакалавр
Освітня програма	Інформаційні системи та технології
Тривалість викладання	11, 12 чверть
Заняття:	весняний семестр
лекції:	2 години
лабораторні заняття:	1 година
Мова викладання	Українська
Форма підсумкового контролю	Іспит

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

Кафедра, що викладає Безпеки інформації та телекомунікацій

Викладач:
Тимофєєв Дмитро Сергійович
старший викладач кафедри

Персональна сторінка
https://bit.nmu.org.ua/ua/pro_kaf/prepods/timofeev.php

E-mail:
tymofieiev.d.s@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. Результати навчання

Основні 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.

– надавати обґрунтований опис систем забезпечення захисту інформації, як складових інформаційних систем, що проектуються.

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

4. Структура курсу

ЛЕКЦІЇ

1. Забезпечення захисту інформації в інформаційно-комунікаційних системах

1.1. Базові поняття

1.2. Будова систем захисту інформації

1.3. Основи криптографічних методів захисту інформації

1.4. Теоретичні основи захисту інформації

2. Основні загрози безпеці інформації в інформаційно-комунікаційних системах

2.1. Типові вразливості систем і аналіз причин їх появи.

2.2. Шкідливе програмне забезпечення

3. Нормативні документи забезпечення безпеки інформації

3.1. Розвиток стандартів безпеки.

3.2. Нормативно - правова база України.

3.3. Міжнародні стандарти

4. Захист інформації на рівні операційної системи

4.1. Апаратне забезпечення засобів захисту

4.2. Захищені операційні системи

4.3. Засоби захисту в операційній системі UNIX

4.4. Засоби захисту в операційній системі Windows

4.5. Системи оброблення конфіденційної інформації

5. Захист інформації в розподілених системах

5.1. Основи безпеки інформації в комп‘ютерних мережах.

5.2. Безпека мережних протоколів інтернету.

5.3. Безпека прикладних служб інтернету.

5.4. Передавання інформації через захищені мережі.

6. Створення, введення в дію та супроводження захищених систем

6.1. Створення комплексної системи захисту інформації

6.2. Супроводження комплексної системи захисту інформації

ЛАБОРАТОРНІ ЗАНЯТТЯ

PR-1 – Оцінка ризиків інформаційної безпеки.

PR-2 – Розробка моделей порушника та загроз.

PR-3 – Розробка політики безпеки інформації в інформаційних системах.

5. Технічне обладнання та/або програмне забезпечення

№ роботи (шифр)	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
PR-1	Оцінка ризиків інформаційної безпеки.	Персональний комп’ютер Платформа MS Windows або Ubuntu MS Office, або MS Office 365 або LibreOffice Калькулятор рисков FAIR-U Пакет DS Office
PR-2	Розробка моделей порушника та загроз.	Персональний комп’ютер Платформа MS Windows або Ubuntu BoUML, MS Office, або MS Office 365 або LibreOffice
PR-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 з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Лабораторна частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
65	30	20	5	**100**

Лабораторні роботи приймаються за контрольними запитаннями до кожної з робот, які або присутні в опису роботи, або відповідають плану лекцій, до яких відноситься лабораторна робота.

Теоретична частина оцінюється за результатами здачі екзаменаційного білету, який 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 на електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

65 балів – дана розгорнута відповідь на два питання.

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

30 балів – два повна відповідь на одне питання або на два питання зі значними помилками.

20 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 лабораторної роботи

З кожної лабораторної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи. Кількість вірних відповідей визначають кількість отриманих 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". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.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 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 «Захист інформації в інформаційно-комунікаційних системах». За участь у анкетуванні здобувач вищої освіти отримує **5 балів**.

8 Рекомендовані джерела інформації

1. Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 − Інформаційні технології, спеціальність 126 − Інформаційні системи та технології. Затверджено Наказом Міністерства освіти і науки України 12.12.2018 р. № 1380. –17с.
2. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
3. 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.
4. 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.
5. Криптологія у прикладах, тестах і задачах : навч. посіб./ Т. В. Бабенко, Г. М. Гулак, С. О. Сушко, Л. Я. Фомичова; М-во освіти і науки України, Держ. вищий навч. закл. “Нац. гірн. ун-т”.- Д.: НГУ, 2013
6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
7. 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)
9. Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua
10. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua
11. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. ДСТСЗІ СБ України, 1999 – 16 с.
12. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТС31 СБ України, 1999. - 26 с.
13. NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4.
14. ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
15. Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
16. CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org