СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ СИСТЕМАХ»

Ступінь освіти	Магістр
Галузь знань	12 Інформаційні технології 17 Електроніка, автоматизація та електронні комунікації
Тривалість викладання	3, 4 чверть
Заняття:	2-йсеместр
лекції:	2 години
практичні заняття:	1 година
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/course/view.php?id=5383

Кафедра, що викладає Кафедра безпеки інформації та телекомунікацій

Викладач:
Ковальова Юлія Вікторівна
Канд. техн. наук,

Персональна сторінка
https://bit.nmu.org.ua/ua/pro_kaf/prepods/kovaleva.php
E-mail:
kovalova.yu.v@nmu.one

1. Анотація до курсу

Курс висвітлює актуальні питання захисту інформації при створенні та використанні розподілених корпоративних інформаційних систем і мереж масштабу підприємства. Особливу увагу приділено проблемам забезпечення інформаційної безпеки електронного бізнесу, електронної комерції та фінансових обмінів через Internet. Обговорюються основні види атак на комп'ютерні мережі, а також методи і засоби захисту локальних і корпоративних мереж від віддалених Internet-атак. Представлені різні типи міжмережевих екранів; даються рекомендації по їх установці і

використанню в залежності від необхідного ступеня захисту локальної мережі. Детально описуються принципи, алгоритми і протоколи сучасних криптографічних засобів захисту інформації. Викладаються основи формування крипто захищені віртуальних тунелів через відкриті комунікації глобальних відкритих мереж типу Internet. Розглянуті питання забезпечення безпечного віддаленого доступу мобільних та віддалених співробітників до локальних мереж свого підприємства**..**

2. Мета та завдання курсу

Мета дисципліни – освоєння дисциплінарних компетенцій, пов'язаних зі створенням та вивченням сучасних розподілених захищених інформаційних систем різного застосування і ступеня складності

Завдання курсудля здобувачів вищої освіти:

- Ознайомитися зпроблемами безпеки для корпоративних інформаційних систем
- Ознайомитисяз методами та алгоритми криптографічного захисту інформації
- Розглянути різні типи та протоколи ідентифікація та аутентифікація
- Навчитися керувати криптографічними ключами
- Розглянути різні класи Технології захисту інформації
- Навчитисястворювати безпечних віртуальних каналів на рівні каналів і сеансів
- Ознайомитися з принципами побудови інфраструктура управління відкритим ключем PKI.
- Вивчити режими роботи корпоративних міжмережевих екранів брандмауера

3. Результати навчання

Володіти інструментами керування захисту інформації в сучасних гетерогенних корпоративних мережах**.**

4. Структура курсу

ЛЕКЦІЇ

1Локалізація завдання комплексного забезпечення безпеки
1. Локалізація завдання. Положення про конфіденційну інформацію в електронному вигляді. Тематична категоризація. Класифікація інформації за рівнем конфіденційності. 2. Способи зберігання конфіденційної інформації. Звідна інформація. Інтелектуальна власність. Неструктурована інформація. Локальні копії.
2. Основні напрямки захисту інформації. Класифікація внутрішніх порушників

1. Основні напрямки захисту. Захист документів. 2. Захист каналів витоку. Моніторинг (аудит) дій користувачів. 3. Класифікація внутрішніх порушників. Необережні. Маніпульовані. Саботажники. Нелояльні. Порушники, мотивовані ззовні. Інші типии порушників.
3.Технології аутентифікації і шифрування в розподілених системах
1. Вимоги до аутентифікації і шифрування. Аутентифікація, заснована на IP-адресі. 2. Basic-аутентифікація. Digest-аутентифікація. SSL / TLS. 3. Можливості SSL / TLS. Слабкімісця SSL / TLS. Приклад SSL / TLS-сесії. Схемишифрування SSL / TLS. Вимоги до реалізації SSL / TLS. 4. Список дій для технологій аутентифікації і шифрування. Firewall прикладного рівня для web - ModSecurity. Взаємодія ModSecurity з пакетним фільтром.
4. Реалізація комплексної безпечної розподіленої мережевої інфраструктури на прикладі web-сервера
1. Топологія мережі. Демілітаризована зона. Хостинг у зовнішні йорганізації. 2. Мережеві елементи. Роутер і firewall. Системи виявлення проникнення (IDS). Мережеві комутатори та концентратори. Список дій для забезпечення безпеки мережевої інфраструктури. 3. Адміністрування web-сервера. Створення логів. Основні можливості створення логів. Додаткові вимоги для створення балок. Можливі параметри логів. Перегляд і зберігання лог-файлів. 4. Автоматизовані інструментальні засоби аналізу лог-файлів. Процедури створення backup web-сервера.

Практичні заняття

1. Дослідження реальних об’єктів інформаційної діяльності
2. Розробкапроцедур сканування корпоративної мережі.
3. Розробка засобів збору інформації на кінцевих точках.
4. Створення плану захисту корпоративної мережі

5. **Технічне обладнання та/або програмне забезпечення**
   Технічні засоби навчання: мультимедійні та комп’ютерні пристрої.
   Програмні засоби дистанційної освіти: MSOffice 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		
55	40	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:

55 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.

10 балів – Достатня зрозумілість відповіді

7 бали – Добра зрозумілість відповіді

4 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. Основи управління інформаційною безпекою: навчальний посібник для вузів / А. П. Куріло [и др.] .— Київ : Телеком, 2014.
5. Захист програмного забезпечення. Частина 2: навчальний посібник / В.А. Каплун, О.В. Дмитришин, Ю.В. Баришев – Вінниця : ВНТУ, 2014 . – 105 с.