СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ СИСТЕМАХ»

Ступінь освіти	Магістр
Освітня програма	Кібербезпека
Тривалість викладання	3, 4 чверть
Заняття:	Весіннійсеместр
лекції:	2 години
лабораторні заняття:	1 година
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: http://do.nmu.org.ua/course/view.php?id=2661

Кафедра, що викладає Кафедра безпеки інформації та телекомунікацій

Викладач:
ФлоровСергій Володимирович
Доцент, канд. техн. наук,

Персональна сторінка
https://bit.nmu.org.ua/ua/pro_kaf/prepods/florov.php**E-mail:**
florov.s.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
- Навчитися сстворювати 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

- Проблеми безпеки Інтернету, електронного бізнесу та корпоративних інформаційних систем.
- Розгортання DNScервісу для корпоративних мереж побудованих на Windowsплатформі
- Проблеми безпеки корпоративних інформаційних систем
- Електронні цифровий підпис
- Ідентифікація та аутентифікація
- Технології захисту інформації
- Створення безпечних віртуальних каналів на рівні каналів і сеансів
- Інфраструктура управління відкритим ключем PKI
- Технологія міжмережевих екранів.
- Технології побудови систем захисту для хмарних корпоративних мереж

5. Технічне обладнання та/або програмне забезпечення

№ роботи (шифр)	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
СР2-1.6 ЗР4-1.6	Створення локального домену	Лабораторія кіберзахисту кафедри БІТ. Локальна мережа. Віртуальні комп'ютери
СР3-1.6 ЗР6-1.6	Організація маршрутизації і віддаленого доступу в середовищі Windows.	Лабораторія кіберзахисту кафедри БІТ. Локальна мережа. Віртуальні комп'ютери.
СР1-СР3-1.6 ЗР3-1.6,	Розгортання міжмережевого екрануMicrosoft Forefront Threat Management Gateway	Лабораторія кіберзахисту кафедри БІТ. Локальна мережа. Віртуальні комп'ютери
СР2-1.6 ЗР4-1.6	Розгортання інфраструктури управління відкритим ключем PKI	Лабораторія кіберзахисту кафедри БІТ. Локальна мережа. Віртуальні комп'ютери
СР1 ЗР4-1.6	Моніторинг серверів та робочих станцій	Аеродинамічна труба. Лазерний тахометр

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
75-89	добре
60-74	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		
66	30	20	4	**100**

Лабораторні роботи приймаються за контрольними запитаннями до кожної з роботи.

Теоретична частина оцінюється за результатами здачі контрольної тестової роботи, яка містить 20 запитань, з яких 17 – прості тести (1 правильна відповідь), 3 задачі.

6.3. Критерії оцінювання підсумкової роботи

17 тестових завдань з чотирма варіантами відповідей, **1** правильна відповідь оцінюється у **3 бали (разом 51 бал)**. Опитування за тестом проводиться з використанням технології Microsoft Forms Office 365.

Задачі наводяться також у системі Microsoft Forms Office 365. Вирішена на папері задача сканується (фотографується) та відсилається на електронну пошту викладача впродовж часу, відведеного на здачу теоретичної частини. Несвоєчасно вислана відповідь враховується такою, що не здана.

Правильно вирішена **задача** оцінюється в 5 балів, причому:

- **5 балів** – відповідність еталону, з одиницями виміру;
- **4 бали** – відповідність еталону, без одиниць виміру або помилками в розрахунках;
- **3 бали** – незначні помилки у формулах, без одиниць виміру;
- **2 бали** – присутні суттєві помилки у рішенні;
- **1 бал** – наведені формули повністю не відповідають еталону;
- **0 балів –** рішення не наведене.

6.4. Критерії оцінювання практичної роботи

З кожної лабораторної роботи здобувач вищої освіти отримує 5 запитань з переліку контрольних запитань. 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 освітим 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 розподілених системах». За участь у анкетуванні здобувач вищої освіти отримує **4 бали**.

8 Рекомендовані джерела інформації

1. Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.] .— 2-е изд., испр .— Москва : Горячаялиния-Телеком, 2014.
2. Информационная безопасность открытых систем : учебник / Д. А. Мельников .— Москва : Флинта : Наука, 2013 .
3. Гольдштейн Б.С. Сети связи: учеб, для вузов / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. - СПб: БХВ-Петербург, 2011.
4. Kiczales G. The Art of Meta-Object Protocol. The MIT Press, 1991. 345 pp.
5. Laddad R., Johnson R. Aspectj in Action: Enterprise AOP with Spring Applications. Manning Publications, 2009. 568 pp.
6. Rashid A. Transactions on Aspect-Oriented Software Development I (Lecture Notes in
7. Computer Science) / A. Rashid, M. Aksit. — Secaucus, NJ, USA: Springer-Verlag New York,
8. Inc., 2006. – 344 pp.
9. Vyncke E. LAN switching security. – Cisco Press, 2008. – 340 p.
10. б) дополнительная литература:
11. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : Пер. с англ. – М. :
12. Издательский дом “Вильямс”, 2003. – 976 с.
13. 10. Томас М. Томас II. Структура и реализация сетей на основе протокола OSPF, 2-е изд. : Пер. с
14. англ. – М. : Издательский дом “Вильямс”, 2004. – 816 с.
15. Хилл Б. Полный справочник по Cisco. : Пер. с англ. – М. : Издательский дом “Вильямс”,2004. – 1078 с.
16. Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst. : Пер. с англ. – М. : Издательский дом “Вильямс”, 2004. – 560 с.
17. Программное обеспечение и Интернет ресурсы:
18. Cisco Systems, Inc. Cisco SAFE reference guide [Электронныйресурс]. – URL: http://cisco.com
19. Cisco Systems, Inc. Enterprise campus 3.0 architecture: overview and framework [Электронныйресурс]. – URL: http://cisco.com/go/srnd.
20. Cisco Systems, Inc. High availability campus network design – routed access layer using EIGRP or OSPF system assurance guide [Электронныйресурс]. – URL: http://cisco.com/go/srnd.