СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Захист інформації в комп'ютерних мережах»

Ступінь освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Тривалість викладання	1 семестр
Заняття:	13 і 14 чверті
лекції	2 год./тижд.
лабораторні роботи	3 год./тижд.
Мова викладання	українська

Передумови для вивчення: Дисципліна «Захист інформації в комп'ютерних мережах» викладається у 7-му семестрі відповідно до навчального плану. Базовими дисциплінами для успішного опанування курсу є наступні: «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування та масштабування корпоративних мереж», «Теорія інформації та кодування», «Операційні системи».

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/course/view.php?id=1663
Консультації: за окремим розкладом, що попередньо погоджений зі здобувачами освіти.
Онлайн-консультації: MS Teams, електронна пошта

Інформація про викладачів:

Викладач:
Олевський Віктор Ісаакович
д-р техн. наук, проф., професор каф. ІТКІ
Посилання на профіль:
Сторінка кафедри ПЗКС:
https://it.nmu.org.ua/ua/HR_staff/prepods/Olevskyi.php
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/1559506
Orcid ID:
https://orcid.org/0000-0003-3824-1013
Scopus ID:
https://www.scopus.com/authid/detail.uri?authorId=56419822400
ResearchGate Profile:
https://www.researchgate.net/profile/Olevskyi-Viktor

1. Анотація курсу

У теперішній час у значної кількості промислових підприємств і бізнес-структур різного профілю та форми власності актуалізується нагальна потреба щодо захисту інформації у комп'ютерних мережах. Такий факт спонукає інженерів і науковців у галузі інформаційних технологій та дотичних із нею на комплексне вирішення задач, що пов'язані з розробкою, впровадженням і технічним супроводом інноваційних програмно-технічних рішень щодо цього питання. Одним із найбільш апробованих і загальновизнаних рішень із комплексного захисту комп'ютерних мереж є концепція фірми CISCO.

Академічний курс «Захист інформації в комп'ютерних мережах» покликаний до формування у студентів знань і вмінь із розуміння та кваліфікованого застосування в практичній діяльності теоретико-прикладних засад захисту комп'ютерних мереж на різних ієрархічних рівнях. Змістовне наповнення вищезазначеної дисципліни розроблено на основні сучасних досягнень фірми CISCO у цей галузі.

Характерною рисою даного курсу є те, що значна частина теоретичної і практичної компонент побудована на основі курсу з безпеки мереж академії CISCO, які у вигляді демонстраційних і навчальних матеріалів інтегровано до лекцій та лабораторних робіт. Значна увага курсу приділена практичній складовій, яка дозволяє отримати навички проєктування й тестування систем захисту інформації у комп'ютерних мережах різного рівня складності та функціонального призначення, що в перспективні надає слухачам цієї дисципліни певні переваги на ринку праці.

2. Мета та завдання навчальної дисципліни

Мета дисципліни – формування знань і навичок щодо фундаментальних теоретичних положень і практичних аспектів із розробки і впровадження програмно-технічних рішень інформаційних технологій щодо забезпечення безпеки в інформаційних мережах. Під час вивчення даної дисципліни у студентів формуються компетентності щодо вирішення теоретико-прикладних завдань різного призначення і рівня складності, які пов'язані з аналізом, синтезом, проєктуванням і технічним супроводом програмно-технічних рішень щодо забезпечення безпеки в інформаційних мережах.

Завдання курсу:

- опанування теоретико-понятійної бази курсу;
- ознайомлення зі сучасною апаратною і програмною базами побудови систем захисту інформації у комп'ютерних мережах;
- опанування засобів і методів протидії отриманню несанкціонованого доступу до інформаційних ресурсів, захисту адміністративного доступу до мережного обладнання в комп'ютерних мережах на різних ієрархічних рівнях;
- ознайомлення зі сучасними перспективними напрямками концепції захисту комп'ютерних мереж фірми CISCO.

3. Результати навчання

Знати, розуміти та вміти використовувати у практичній діяльності:

- склад і принципи функціонування систем захисту інформації, методи захисту інформації у комп'ютерних мережах;
- законодавчу та нормативно-правову базу, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності;
- знання про кіберзлочинців, типові загрози, атаки та області їх розповсюдження, категорії вразливостей програмного та апаратного забезпечення і систем безпеки, наслідки кібератак;
- основні поняття криптографії, алгоритмів шифрування, основні напрями сучасної криптографії, криптографічні системи для забезпечення конфіденціальності даних в інформаційних мережах;
- заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів, захисту адміністративного доступу до мережного обладнання в комп'ютерних мережах;
- практичні навички з впровадження моделі AAA на мережевих пристроях, технології міжмережевих екранів для захисту периметра мережі, налаштування IPS для нейтралізації атак на мережу;
- систему запобігання вторгнень (IPS) безпечні віртуальні приватні мережі (VPN) .

4. Структура курсу

Види та тематика навчальних занять	Обсяг складових, *години*
ЛЕКЦІЇ	**44**
Вступ Мета і завдання дисципліни « Захист інформації в комп'ютерних мережах». Основні поняття та визначення. Загальна схема процесу забезпечення безпеки. Загальнодержавна правова база захисту інформації в інформаційних системах. Основні кіберзакони, стандарти та відповідальність. Інтернет-спільноти з кібербезпеки.	4
Тема 1. Кібербезпека – загрози, вразливості та атаки Типові загрози, атаки та області їх розповсюдження. Характеристика сучасних кібератак на інформаційно-комунікаційні технології. Інструменти і процедури для нейтралізації наслідків впливу шкідливого ПЗ та поширених мережевих атак.	4
Тема 2. Процедури забезпечення безпеки. Фізичний захист. Поточні виправлення й оновлення. Антивірусне ПЗ. Антиспам. Програма захисту від шпигунського і рекламного ПО. Засоби блокування спливаючих вікон. Захист даних. Безпека бездротових пристроїв.	4
Тема 3. Криптографічні методи захисту інформації при її передаванні у комп'ютерних мережах Історичний розвиток криптографії та криптоаналітики. Поняття шифру та коду. Симетричні криптосистеми шифрування. Основні режими роботи та особливості застосування блочного симетричного алгоритму. Алгоритм шифрування DES. Американський стандарт шифрування AES. Схема Фейстеля. Шифр Blowfish.	4
Тема 4. Асиметричні шифри. Розподілення ключів по схемі Діффі-Хеллмана. Криптографічна система RSA. Криптографічна система Эль-Гамаля. Сумісне використання симетричних та асиметричних шифрів.	4
Тема 5. Методи шифрування інформації. Застосування алгоритмів шифрування для забезпечення конфіденційності даних. Шифрування інформації методом з відкритим ключем.	4
Тема 6. Забезпечення безпеки мережевих пристроїв Захист мережевої інфраструктури. Підходи до захисту граничних маршрутизаторів. Забезпечення захисту адміністративного доступу. Безпечний локальний і віддалений доступ.	4
Тема 7. Технологія захисту ААА. Налаштування засобів ААА сервера мережевого доступу. Архітектура захисту ААА. Призначення ААА. Локальна та групова політики безпеки системи. Локальна автентифікація ААА. Характеристики та протоколи ААА на основі сервера. Впровадження серверної автентифікації за допомогою протоколів TACACS+ і RADIUS. Серверна авторизація та облік ААА.	4
Тема 8. Впровадження технологій міжмережевого екрану для захисту периметра мережі Списки контроля доступом. Технології міжмережевих екранів. Зональні міжмережеві екрани (Zone Based Firewal)	4
Тема 9. Впровадження системи запобігання вторгненням (IPS) Методи виявлення вторгнень. Характеристики IDS і IPS. Впровадження IPS. Сігнатури IPS.	4

Види та тематика навчальних занять	Обсяг складових, *години*
Тема 10. Впровадження захищених приватних віртуальних мереж (VPN) Призначення і типи мереж VPN. Загальні відомості про IPsec. Компоненти мережі IPsec VPN та їх функціонування. Реалізація мереж Site-to-Site IPsec VPN.	4
ЛАБОРАТОРНІ РОБОТИ	**67**
Лабораторна робота 1. Дослідження відомостей про атаки	7
Лабораторна робота 2. Дослідження процесу шифрування повідомлення з допомогою таблиці Віженера	8
Лабораторна робота 3. Дослідження алгоритму шифрування та системи цифрового підпису Ель Гамаля	8
Лабораторна робота 4. Налаштування безпечного адміністративного доступу обладнання Cisco для захисту від злому	7
Лабораторна робота 5. Захист адміністративного доступу за допомогою AAA та протоколу RADIUS	7
Лабораторна робота 6. Налаштування ACL з метою запобігання атакам	8
Лабораторна робота 7. Налаштування системи запобігання вторгнень (IPS)	8
Лабораторна робота 8. Захист міжмережевих з'єднань Zone-Based Policy Firewall	7
Лабораторна робота 9. Налаштування та перевірка Site-to-Site IPsec VPN	7
РАЗОМ	**120**

5. Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.
Засоби дистанційної освіти: Moodle, MS Teams.
Засоби дистанційної освіти: Moodle, MS Teams.
Пакети приладних програм:

- MS Office;
- Cisco Packet Tracer (безкоштовний для студентів академії Cisco);
- клієнтське програмне забезпечення SSH, наприклад PuTTy або Tera Term, для виконання лабораторних на мережному обладнанні.

Мережне обладнання:

- 3 маршрутизатори Cisco, 2 ліцензії Security Technology Package;
- 3 двопортові плати послідовного інтерфейсу WAN;
- 3 комутатора Cisco;
- один багатофункціональний пристрій безпеки Cisco ASA;
- різні кабелі Ethernet.

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. Здобувач ступеня освіти «Бакалавр» 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 успішності за теоретичну частину курсу (максимум – 36 балів) та оцінок за виконання лабораторних робіт (максимум 8 балів за кожну роботу та максимальною сумарною оцінкою за всі роботи – 64 бали). Отримані бали за теоретичну частину курсу та практичні роботи додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Шкала оцінювання (зазначено максимально можливі бали):

Теоретична частина	**Лабороторні роботи**		**Разом**
	При своєчасному складанні	При несвоєчасному складанні	
36	64	40	100

6.3 Критерії оцінювання поточного та підсумкового контролю:

– підсумкове оцінювання відбувається у формі заліку у форматі тесту, який складається з 16 завдань (15 запитань із вибором варіанту відповіді – 2 бали за правильну відповідь; 1 завдання у формі задачі – максимум 6 балів, якщо надано повністю правильну і обґрунтовану відповідь);

– поточне оцінювання лабораторних робіт відбувається шляхом захисту звіту з відповідної роботи (максимальний бал – 8, який формується наступним чином: 50 % – правильність і повнота викладення матеріалу в звіті, 50 % – захист індивідуальної роботи шляхом відповіді на контрольні питання).

7. Політика курсу

7.1. Політика щодо академічної доброчесності. Академічна доброчесність студентів 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 НТУ «Дніпровська політехніка» 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 студентом 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. Студенти повинні мати активовану університетську (корпоративну на домені @nmu.one) 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 студентів денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, відрядження, які необхідно підтверджувати документами у разі тривалої (два тижні) відсутності. Про відсутність на занятті та причини відсутності студент має повідомити викладача або особисто, або через старосту. Якщо студент захворів, ми рекомендуємо залишатися вдома і навчатися за допомогою дистанційної платформи. Студентам, чий стан здоров'я є незадовільним і може вплинути на здоров'я інших студентів, буде пропонуватися залишити заняття (така відсутність вважатиметься пропуском з причини хвороби). Лабораторні заняття не проводяться повторно, ці оцінки неможливо отримати під час консультації. **За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.**

7.5. Участь в анкетуванні. Наприкінці вивчення курсу та перед початком сесії студентам буде запропоновано анонімно заповнити електронні анкети (MS 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.

8. Рекомендовані джерела інформації

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах: навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.
2. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологія і мережах [Електронний ресурс] : навч. посіб. дл студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.
3. Курс мережевої академії Cisco: Network Security, 2022. Режим доступу. [URL: **https://www.netacad.com/courses/cybersecurity/network-security**]
4. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В.Гайворонський, О.М. Новіков.–К.: Видавнича група BHV,2009. –608 с., іл
5. Юдін О.К., Конахович Г.Ф., Корченко О.Г., Захист інформації в мережах передачі даних: підручник/О.К. Юдін, Г.Ф.Конахович, О.Г.Корченко. –К.:Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. –714с., іл.
6. Богуш В.М., Довидьков О.А. Основи захищених інформаційних технологій/ В.М.Богуш, О.А.Довидьков. –К.: ДУІКТ, 2005. – 450 с.
7. Kizza J. M. Guide to Computer Network Security Springer. Series Title: Computer Communications and Networks, London 2015, 545 p. https://doi.org/10.1007/978-1-4471-6654-2
8. Olifer V. G., Olifer N. A. Computer networks: principles,technologies and protocols for network. Wiley India Pvt. Limited, ISBN 8126509171, 2006 – 1000 p.
9. Miller, A. R. The Cryptographic Mathematics of Enigma, Center for Cryptologic History National Security Agency [Электронний ресурс] / A. R. Miller // Google Диск. – 2019. – Режим доступу: https://drive.google.com/file/d/1By1nea1BhIiNwCfykdmQAawkyh5QT_hr/view.
10. Soni, A., Upadhyay, R., Jain, A. (2017). Internet of Things and Wireless Physical Layer Security: A Survey. In: Satapathy, S., Bhateja, V., Raju, K., Janakiramaiah, B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks and Systems, vol 5. Springer, Singapore. **https://doi.org/10.1007/978-981-10-3226-4_11**
11. Shivanna, K., Deva, S.P., Santoshkumar, M.. Privacy Preservation in Cloud Computing with Double Encryption Method. In: Satapathy, S., Bhateja, V., Raju, K., Janakiramaiah, B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks

and Systems, vol 5. Springer, Singapore, (2017) **https://doi.org/10.1007/978-981-10-3226-4_12.**

12. Фонд нормативних документів у сфері технічного та криптографічного захисту інформації в Україні. Режим доступу. [URL: **https://cip.gov.ua/ua/news/perelik-dokumentiv-normativno-pravovoyi-bazi-sho-zabezpechuye-nadannya-vidpovidnikh-vidiv-poslug-u-galuzi-kriptografichnogo-zakhistu-informaciyi-krim-poslug-elektronnogo-cifrovogo-pidpisu**