Силабус навчальної дисципліни
«КОРПОРАТИВНІ МЕРЕЖІ ТА СИСТЕМИ ДОСТУПУ»

Спеціальність	*125 Кібербезпека*
Освітня програма	*Кібербезпека*
Освітній рівень	*бакалавр*
Статус дисципліни	*вибіркова*
Мова викладання	*Українська*
Курс / семестр	*3 / 5 семестр*
Кількість кредитів ЄКТС	*7*
Розподіл за видами занять та годинами навчання	*Лекції – 34 год.* *Лабораторні – 34 год.* *Самостійна робота – 142 год.*
Форма підсумкового контролю	*Екзамен*
Кафедра	*Кібербезпеки та інформаційних технологій, м. Харків, пр-т Науки 9-А, 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Викладач (-і)	*Євсеєв Сергій Петрович, д.т.н., проф.*
Контактна інформація викладача (-ів)	*erhii.yevseiev@hneu.net*
Дні занять	*П'ятниця*
Консультації	*П'ятниця 13.55; дистанційні; відповідно до графіку; індивідуальні*

Мета навчальної дисципліни: "*Корпоративні мережі та системи доступу*" є надання комплексу знань в області захисту комп'ютерних мереж, ознайомлення з системами й методами визначення захищеності програмних продуктів в комп'ютерних мережах та системах доступу, набуття на основі цих знань практичних навичок і теоретичних знань, необхідних для творчого підходу в питанні сучасного та в майбутньому оперативного захисту контуру бізнес-процесів в корпорації.

Передумови для навчання

Менеджмент інформаційної безпеки, Основи криптографічного захисту, Технології програмування

Тема 1. Сучасні загрози мережевої безпеки. Забезпечення безпеки мереж. Нейтралізація загроз

Тема 2. Забезпечення безпеки мережевих пристроїв. Захист доступу до пристроїв. Призначення адміністративних ролей. Моніторинг пристроїв і керування ними. Використання автоматичних функцій забезпечення безпеки. Захист площини управління.

Тема 3. Автентифікація, авторизація та облік. Призначення AAA. Локальна автентифікація AAA. Серверна AAA. Серверна автентифікація AAA. Серверна авторизація та облік.

Тема 4. Впровадження технологій брандмауера. Технології брандмауера. Зональні міжмережеві екрани.

Тема 5. Впровадження системи запобігання вторгнень. Технології IPS. Сигнатури IPS. Впровадження системи IPS

Тема 6. Забезпечення безпеки локальної мережі (LAN). Безпека кінцевих пристроїв.

Загрози безпеці на 2-му рівні

Тема 7. Криптографічні системи. Криптографічні сервіси. Базові відомості про цілісність і автентифікації. Конфіденційність. Криптографія з відкритими ключами

Тема 8. Впровадження віртуальних приватних мереж (VPN). Мережі VPN. Компоненти і принципи роботи IPsec VPN. Впровадження мереж IPsec VPN за схемою Site-to-Site (VPN між двома пунктами) з використанням інтерфейсу командного рядка (CLI).

Тема 9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA). Знайомство з ASA. Конфігурація брандмауера ASA.

Тема 10. Багатофункціональний пристрій захисту Cisco (Adaptive Security Appliance, ASA) з розширеною функціональністю. ASA Security Device Manager. Конфігурація VPN на ASA.

Тема 11. Управління безпечної мережею. Тестування безпеки мережі. Розробка комплексної політики безпеки.

Матеріально-технічне (програмне) забезпечення дисципліни

TrueCrypt 6.1, КриптоБанк 5.0, EDI-системи, First Virtual

Сторінка курсу на платформі Moodle (персональна навчальна система) Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Корпоративні мережі та системи доступу" https://pns.hneu.edu.ua/course/view.php?id=7524.	*Посилання:*

Рекомендовані джерела

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);

2. Закон України “Про захист персональних даних” (2010)

3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)

4. Закон України “Про національну безпеку (2018)

5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)

6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;

7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;

8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.

11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних

системах від несанкціонованого доступу.

12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.

15. ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.

16. ISO/IEC 27002. "Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью."

17. ISO/IEC 27005. "Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности

18. http://bezopasnost.biz

19. http://dstszi.gov.ua

20. www.itsec.ru Інтернет-журнал «Інформаційна безпека».

21. www.inside-zi.ru Інформаційно-методичний журнал «Захист інформації.

Система оцінювання результатів навчання

*Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності та екзаменом, дорівнює або перевищує 60. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.*

Більш детальна інформація щодо оцінювання наведена в технологічній карті дисципліни.

Накопичування рейтингових балів з навчальної дисципліни *(приклад)*

Види навчальної роботи	**Мах кількість балів**
Лекції	**12**
Захист лабораторних робіт	**24**
Поточні контрольні роботи	**24**
Екзамен	**40**
Максимальна кількість балів	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та ХНЕУ ім. С. Кузнеця

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену (іспиту), диференційованого заліку, курсового проекту (роботи), практики, тренінгу	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	

74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

Політики навчальної дисципліни

Політика дотримання академічної доброчесності,
Політика щодо пропусків занять,
Політика щодо виконання завдань пізніше встановленого терміну,
тощо

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни «Корпоративні мережі та системи доступу», 2020.

Силабус затверджено на засіданні кафедри «31»серпня 2020 р. Протокол №2