



МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ

Факультет № 4
Кафедра протидії кіберзлочинності

ЗАТВЕРДЖЕНО

На спільному засіданні кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
протокол № 2 від 22.06.2023

Завідувач кафедри

Олександр МАНЖАЙ

БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ (ОК.17)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	Носов Віталій Вікторович , професор кафедри протидії кіберзлочинності факультету № 4, кандидат технічних наук, доцент E-mail: vitnos@univd.edu.ua Лекційний потік: факультет № 4, Ф4-302, 402
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації

Статус дисципліни	Нормативна компонента освітньо-наукової програми, вивчається в 5, 6 семестрах 3 курсу навчання та 7 семестрі 4 курсу навчання
Мета вивчення дисципліни	формування знань і вмінь забезпечувати кібернетичну безпеку в інформаційних та комунікаційних системах
Завдання вивчення дисципліни	<ul style="list-style-type: none"> - ознайомлення із різними видами кібератак, методами і засобами забезпечення кібербезпеки в інформаційно-комунікаційних системах; - формування навичок аналізу можливих кіберзагроз, впровадження та експлуатація засобів і сервісів кібербезпеки в інформаційно-комунікаційних системах.
Обсяг дисципліни в кредитах ECTS/годинах	11 кредитів ECTS (загальний обсяг – 330 год.) 3 них (денна/заочна):
	- аудиторна робота: 160/32 год.
	- самостійна робота: 170/298 год.
Форми та види проведення навчальних занять	Форма навчання – денна/заочна Види навчальних занять: - лекції: 72/10 год.; - лабораторні заняття: 88/22 год.
Самостійна робота	Опрацювання рекомендованої літератури, виконання домашніх завдань до лабораторних занять, виконання індивідуальних завдань до лабораторних занять та курсової роботи
Індивідуальні завдання	Наукові доповіді, індивідуальні завдання до лабораторних занять
Необхідне обладнання	Мультимедійне обладнання (ноутбук, проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	<p>Методи контролю: поточний та підсумковий контроль (залік, екзамен)</p> <p>Форми контролю: захист індивідуальних завдань на лабораторних заняттях, тестування, перевірка аудиторних контрольних робіт, перевірка виконання самостійних робіт, захист курсової роботи.</p> <p>Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням.</p>
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що

	<p>характеризується комплексністю та неповною визначеністю умов</p> <p>ЗК 2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.</p>
Фахові компетентності (ФК)	<p>ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах</p> <p>ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки</p> <p>ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та і походження</p> <p>ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p> <p>ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки</p>

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

Тема №1. Основні відомості про кібербезпеку

Терміни та визначення. Умови безпеки інформації. Поняття кіберпростору. Базова технічна модель безпеки інформаційних технологій. Зменшення інформаційних ризиків. Загальна структура інформаційно-телекомунікаційних систем (ІТС). Архітектура безпеки ІТС. Застосування сервісів безпеки до рівнів безпеки ІТС. Типи атак на інформаційні системи. Принципи захисту від атак.

Тема №2. Пасивний збір інформації

Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Побудова та аналіз зв'язків між частинами отриманої інформації. Способи протидії пасивному збору інформації.

Тема №3. Активний збір інформації про мережу

Основні протоколи стеку TCP/IP. Побудова схеми мережі. Засоби для отримання інформації щодо вузлів та сервісів у мережі. Пошук вразливостей та інструменти сканування вузлів мережі на вразливості. Отримання інформації з сервісів: NetBIOS, LDAP, SMTP, DNS.

Тема №4. Аналіз трафіку в комп'ютерних мережах

Механізми перехоплення трафіку в комп'ютерних мережах; використання програм для перехоплення та аналізу трафіку; атаки в локальній мережі та захист від них: протоколи ARP та DHCP, переповнення таблиці комутації, ARP підміна, підміна DHCP; Атака отруєння DNS та захист від неї.

Використання програм для перехоплення та аналізу трафіку; засоби для MAC затоплення, ARP підмини; засоби для атаки на DHCP; створення підробленого DHCP серверу.

Тема №5. Перехоплення сесій передачі даних в комп'ютерних мережах

Механізми перехоплення сесій. Типи перехоплення сесій. Перехоплення сесії на транспортному та прикладному рівнях. Інструменти для захоплення сесій прикладного та транспортного рівнів, відображення та аналіз отриманої інформації.

Використання інструментів для перехоплення сесій прикладного та мережного рівнів; використання інструментів для відображення та аналізу отриманої інформації.

Тема №6. Безпека в безпроводних мережах

Збір інформації про безпроводні мережі. Шифрування та автентифікація в безпроводних мережах. Атака на безпроводні мережі. Засоби захисту від безпроводних атак.

Тема №7. Безпека в операційних системах

Організація контролю доступу в ОС. Руткити та шпигунські програми. Інструменти, що використовуються для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи.

Тема №8. Шкідливе програмне забезпечення

Типи шкідливого ПЗ. Принципи створення та аналізу троянських програм. Принципи створення та аналізу вірусів. Протидія і виявлення троянських програм, черв'яків та вірусів. Шкідливе ПЗ для мобільних пристроїв з ОС: iOS, Android.

Тема №9. Переповнення буферу

Поняття стеку та купи. Причини виникнення переповнення буферу. Захист від переповнення буферу. Запобігання виконанню даних.

Тема №10. Безпека веб-серверів та веб-застосувань

Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Види атак на веб-застосування. Механізми захисту веб-серверів та веб-застосувань. ПЗ для сканування веб-серверів та веб-застосувань на вразливості.

Тема №11. Атака «відмова в обслуговуванні»

Механізми DoS/DDoS атак. Об'єкти DoS атак. Види DoS атак. Захист від DoS/DDoS атак.

Тема 12. SQL-ін'єкції

Короткий огляд мови SQL. Інструменти для підключення до SQL-сервера та роботи з SQL. Типи SQL-ін'єкцій. Способи виконання SQL-ін'єкцій. Причини виникнення вразливостей, пов'язаних з SQL-ін'єкціями. Захист від SQL-ін'єкцій. Інструменти для автоматичного пошуку вразливостей, пов'язаних з SQL-ін'єкціями.

Тема №13. Соціальна інженерія

Техніки соціальної інженерії. Заходи протидії.

Тема №14. Тестування на вразливість до атак

Методика оцінки вразливостей. Тестування на вразливості. Сканери вразливостей. Послідовність дій при виконанні тестування вебсерверів та вебзастосовувань на вразливість до атак згідно з OWASP.

Тема №15. Сервіси та механізми захисту інформаційно-комунікаційних систем

Процедури ідентифікації, автентифікації, авторизації користувачів. Резервування інформації та компонентів ІКС.

Антивірусні системи, міжмережеві екрани. Системи виявлення та запобігання вторгненням. Мережні пастки. Обхід механізмів захисту IPS, IDS.

Системи контролю та управління доступом. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

Організаційно-технічні заходи відновлення функціонування ІКС. Журнали аудиту подій. Політики резервного копіювання даних.

Моніторинг процесів функціонування ІКС: джерела інформації про події та типи подій, що аналізуються в системах моніторингу; система візуалізації та управління подіями (SIEM); аналіз подій. Платформи ідентифікації актуальних кіберзагроз (MISP).

Віртуальні приватні мережі (VPN). Протоколи автентифікації RADIUS. Протоколи SSL/TLS.

Програмні результати навчання (ПРН)

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів із відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

	ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
	ПРН 19. Застосовувати теорії та методи захисту щодо забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
	ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів у інформаційно-телекомунікаційних системах.
	ПРН 21. Вирішувати задачі забезпечення та супроводу (у.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
	ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та\або кібербезпеки.
	ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
	ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових
	ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів
	ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
	ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в

	ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки
	ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
	ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
	ПРН 31. Застосовувати теорії та методи захисту щодо забезпечення безпеки елементів інформаційно-телекомунікаційних систем
	ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем із використанням процедур резервування згідно встановленої політики безпеки
	ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
	ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
	ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів
	ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
	ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
	ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

		ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.	
		ПРН 52. Використовувати інструментарій щодо моніторингу процесів в інформаційно-телекомунікаційних системах	
		ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз	
Критерії оцінювання результатів навчання		Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:	
		<ul style="list-style-type: none">● поточний контроль - 50 балів;● підсумковий контроль - 50 балів.	
		Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менше 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: захист звітів лабораторних робіт з коефіцієнтом 5.	
		Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (заліку, екзамені).	
ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS			
Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно («зараховано»)	А	«Відмінно» – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою
94-96			
90-93			

85-89	Добре («зараховано»)	В	« Дуже добре » – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками
80-84			
75-79		С	« Добре » – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками
70 – 74	Задовільно («зараховано»)	Д	« Задовільно » – теоретичний зміст курсу освоєний не повністю, але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками
65 – 69			
60 – 64		Е	« Достатньо » – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки
40 – 59	Незадовільно («не зараховано»)	FX	« Умовно незадовільно » – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21 – 40			
1–20		Ф	« Безумовно незадовільно » – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над

		матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки
Перелік питань, що виносяться на підсумковий контроль		
<ol style="list-style-type: none"> 1. Терміни та визначення в області забезпечення кібербезпеки. 2. Об'єкт захисту при забезпеченні кібербезпеки. 3. Принципи безпеки. 4. Загрози кібербезпеки і вектори атаки. 5. Типи кібератак. 6. Механізми забезпечення кібербезпеки. 7. Базова технічна модель ІТ-безпеки. 8. Архітектура безпеки ІТС. 9. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. 10. Побудова та аналіз зв'язків між частинами інформації, що отримана при пасивному зборі інформації про об'єкт кібератаки. 11. Способи протидії пасивному збору інформації про об'єкт кібератаки. 12. Основні протоколи стеку TCP/IP. 13. Побудова схеми комп'ютерної мережі за результатами пасивного збору інформації про об'єкт кібератаки. 14. Засоби для отримання інформації щодо вузлів та сервісів у комп'ютерній мережі. 15. Пошук вразливостей та інструменти сканування вузлів комп'ютерної мережі на вразливості. 16. Отримання інформації з сервісів: NetBIOS, LDAP, SMTP, DNS. 17. Механізми перехоплення трафіку в комп'ютерних мережах. 18. Атаки в локальній мережі та захист від них: атаки на протоколи ARP та DHCP, переповнення таблиці комутації, ARP підміна, підміна DHCP. 19. Атака отруєння DNS та захист від неї. 20. Механізми перехоплення сесій. 21. Типи перехоплення сесій. 22. Перехоплення сесії на транспортному та прикладному рівнях. Протоколи IPsec, SSL/TLS. 23. Збір інформації про безпроводні мережі. 24. Шифрування та автентифікація в безпроводних мережах. 25. Атака на безпроводні мережі. 26. Засоби захисту від безпроводних атак. 27. Організація контролю доступу в ОС. 28. Руткити та шпигунські програми. 29. Протидія атакам на операційні системи. 30. Типи шкідливих програм. 31. Принципи створення та аналізу троянських програм. 32. Принципи створення та аналізу вірусів. 		

33. Протидія і виявлення троянських програм, черв'яків та вірусів. Шкідливі програми для мобільних пристроїв.
34. Поняття стеку та купи в контексті переповнення буферу.
35. Захист від переповнення буферу.
36. Вразливості веб-серверів та веб-застосунків.
37. Види атак на веб-сервер.
38. Види атак на веб-застосування.
39. Механізми захисту веб-серверів та веб-застосунків.
40. Механізми DoS/DDoS атак.
41. Захист від DoS/DDoS атак.
42. Типи та способи виконання SQL-ін'єкцій.
43. Захист від SQL-ін'єкцій.
44. Інструменти для автоматичного пошуку вразливостей, пов'язаних з SQL-ін'єкціями.
45. Техніки соціальної інженерії та заходи протидії.
46. Послідовність дій при виконанні тестування веб-серверів та веб-застосунків на вразливість до атак згідно з OWASP.
47. Процедури ідентифікації, автентифікації, авторизації користувачів.
48. Резервування інформації та компонентів ІКС.
49. Антивірусні системи, міжмережеві екрани.
50. Системи виявлення та запобігання вторгненням.
51. Мережні пастки.
52. Обхід механізмів захисту IPS, IDS.
53. Системи контролю та управління доступом.
54. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
55. Організаційно-технічні заходи відновлення функціонування ІКС.
56. Журнали аудиту подій.
57. Політики резервного копіювання даних.
58. Моніторинг процесів функціонування ІКС:
59. Платформи ідентифікації актуальних кіберзагроз (MISP).
60. Віртуальні приватні мережі (VPN).
61. Протоколи автентифікації RADIUS.
62. Протоколи SSL/TLS.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Кібербезпека для спеціальних агентів кіберполіції (лекції). OSCE. 2016.
2. Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
3. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПП ім. Ігоря Сікорського. – Київ : КПП ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Allen L., Cardwell K. Advanced Penetration Testing for Highly-Secured Environments. Second edition. — Packt Publishing, 2016.
2. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. <https://doi.org/10.6028/NIST.SP.800-53r5>.

Інформаційні ресурси в Інтернеті:

1. <https://csrc.nist.gov/>
2. <https://attack.mitre.org/>
3. <https://owasp.org/www-project-top-ten/>
4. <https://app.hackthebox.com/>
5. <https://www.root-me.org/>
6. <https://tryhackme.com/hackactivities?tab=practice>