МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету №4

РОБОЧА ПРОГРАМА

навчальної дисципліни "Безпека інформаційно-комунікаційних систем"
обов'язкових компонент
освітньої програми першого рівня вищої освіти
"Кібербезпека (безпека інформаційних та комунікаційних систем)"

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол №7 від 30.08.2023

СХВАЛЕНО
Вченою радою факультету №4
Протокол № 8 від 16.08.2023

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол №7 від 29.08.2023

Розглянуто на засіданні кафедри протидії кіберзлочинності (протокол № 19 від 15.08.2023)

Розробник: професор кафедри протидії кіберзлочинності ХНУВС, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Опис навчальної дисципліни

Найменування показників	**Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 12 Загальна кількість годин – 360 Кількість тем – 16	12 Інформаційні технології 125 Кібербезпека бакалавр	Навчальний курс 3,4 Семестри 5,6,7 Види підсумкового контролю: - залік у семестрі 5,6 - екзамен у семестрі 7.

Розподіл навчальної дисципліни за видами занять:

денна форма навчання	заочна форма навчання
Семестр 5: Лекції – 20 год; Лабораторні заняття - 24 год; Самостійна робота – 46 год; Індивідуальні завдання: Реферати (тощо) – 1 Семестр 6: Лекції – 26 год; Лабораторні заняття - 24 год; Самостійна робота – 60 год; Індивідуальні завдання: Курсова робота – 1 Семестр 7: Лекції – 26 год; Лабораторні заняття - 30 год; Самостійна робота – 94 год; Індивідуальні завдання: Реферати (тощо) – 1	Семестр 5: Лекції – 2 год; Лабораторні заняття - 6 год; Самостійна робота – 82 год; Індивідуальні завдання: Реферати (тощо) – 1 Семестр 6: Лекції – 4 год; Лабораторні заняття - 8 год; Самостійна робота – 108 год; Індивідуальні завдання: Курсова робота – 1 Семестр 7: Лекції – 4 год; Лабораторні заняття - 8 год; Самостійна робота – 108 год; Індивідуальні завдання: Реферати (тощо) – 1

2. Мета та завдання навчальної дисципліни

Мета: формування знань і вмінь забезпечувати кібернетичну безпеку в інформаційних та комунікаційних системах (ІКС).

Завдання:

- ознайомлення із різними видами атак на ІКС і способами захисту від них;
- формування навичок аналізу можливих кіберзагроз, впровадження та експлуатація сервісів і засобів безпеки ІКС.

Міждисциплінарні зв'язки: спирається на Вищу математику, Основи кібербезпеки, Інформаційні та комунікаційні технології, Операційні системи та комп'ютерні мережі, Теорія інформації та кодування; забезпечує Управління та організація систем захисту інформації, Цифрова криміналістика.

Очікувані результати навчання:

знати: різні види атак на ІКС та способи і засоби захисту від них;

вміти: аналізувати можливі кіберзагрози загрози, впроваджувати та управляти сервісами безпеки ІКС.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов	
Загальні компетентності (ЗК)	ЗК 2	Знання та розуміння предметної області та розуміння професії
	ЗК 5	Здатність до пошуку, оброблення та аналізу інформації
Фахові компетентності спеціальності (ФК)	ФК 2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки
	ФК 3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах
	ФК 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки
	ФК 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та і походження
	ФК 11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки
	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

3. Програма навчальної дисципліни

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 підміни; 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 безпровідних мережах

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

Тема №7. Безпека в операційних системах

Організація контролю доступу в ОС**.** Руткіти 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 веб-застосувань на вразливість до атак згідно з OWASP.

Тема №15. Сервіси та механізми захисту мережі

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.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №5						
Тема №1. Основні відомості про кібербезпеку	16	6		2	8	залік
Тема №2. Пасивний збір інформації	24	4		8	12	
Тема №3. Активний збір інформації про мережу	24	4		8	12	
Тема №4. Аналіз трафіку в комп'ютерних мережах	16	4		4	8	
Тема №5. Перехоплення сесій передачі даних в комп'ютерних мережах	10	2		2	6	
Всього за семестр №5	**90**	**20**		**24**	**46**	
Семестр №6						
Тема №6. Безпека в безпровідних мережах	24	6		6	12	залік
Тема №7. Безпека в операційних системах	28	6		8	14	
Тема №8. Шкідливе програмне забезпечення	24	6		6	12	
Тема №9. Переповнення буферу	8	2		2	4	
Тема №10. Безпека веб-серверів та веб-застосувань	36	6		12	18	
Всього за семестр №6	**120**	**26**		**34**	**60**	
Семестр №7						
Тема №11. Атака «відмова в обслуговуванні»	16	2		4	10	екз.
Тема №12. SQL-ін'єкції	40	6		10	24	
Тема №13. Соціальна інженерія	24	4		6	14	
Тема №14. Тестування на вразливість до атак	26	2		4	20	
Тема №15. Сервіси та механізми захисту мережі	44	12		6	26	
Всього за семестр №7	**150**	**26**		**30**	**94**	
Всього за дисципліною	**360**	**72**		**88**	**200**	

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №5						
Тема №1. Основні відомості про кібербезпеку	16	1			15	залік
Тема №2. Пасивний збір інформації	24	1		1	22	
Тема №3. Активний збір інформації про мережу	24	1		1	22	
Тема №4. Аналіз трафіку в комп'ютерних мережах	16	1		1	14	
Тема №5. Перехоплення сесій передачі даних в комп'ютерних мережах	10			1	9	
Всього за семестр №5	**90**	**4**		**4**	**82**	
Семестр №6						
Тема №6. Безпека в безпровідних мережах	24	1		1	22	залік
Тема №7. Безпека в операційних системах	28	1		1	26	
Тема №8. Шкідливе програмне забезпечення	24	1		1	22	
Тема №9. Переповнення буферу	8	1		1	6	
Тема №10. Безпека веб-серверів та веб-застосувань	36	2		2	32	
Всього за семестр №6	**120**	**6**		**6**	**108**	
Семестр №7						
Тема №11. Атака «відмова в обслуговуванні»	16	1		1	14	екз.
Тема №12. SQL-ін'єкції	40	1		2	37	
Тема №13. Соціальна інженерія	24	1		1	22	
Тема №14. Тестування на вразливість до атак	26	1		1	24	
Тема №15. Сервіси та механізми захисту мережі	44	2		1	41	
Всього за семестр №7	**150**	**6**		**6**	**138**	
Всього за дисципліною	**360**	**16**		**16**	**328**	

4.1.2. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема №1. Основні відомості про кібербезпеку	
Відпрацювати лекцію за темою. Встановити на власному комп'ютері Kali Linux	2-3
Тема №2. Пасивний збір інформації	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю методів і засобів пасивної розвідки	2-3, ресурси Internet
Тема №3. Активний збір інформації про мережу	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю методів і засобів активної розвідки	2-3, ресурси Internet
Тема №4. Аналіз трафіку в комп'ютерних мережах	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю засобів аналізу трафіку в комп'ютерних мережах для різних ОС	2-3, ресурси Internet
Тема №5. Перехоплення сесій передачі даних в комп'ютерних мережах	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю засобів перехоплення сесій передачі даних в комп'ютерних мережах для різних ОС	2-3, ресурси Internet
Тема №6. Безпека в безпровідних мережах	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю відомих методів і засобів атак на безпровідні мережі	2-3, ресурси Internet
Тема №7. Безпека в операційних системах	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю відомих методів і засобів атак на різні ОС	2-3, ресурси Internet
Тема №8. Шкідливе програмне забезпечення	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю найбільш популярних антивірусних застосувань для різних ОС	2-3, ресурси Internet
Тема №9. Переповнення буферу	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю актуальних атак переповнення буферу	2-3, ресурси Internet
Тема №10. Безпека веб-серверів та веб-застосувань	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю актуальних засобів захисту веб-серверів та веб-застосувань	2-3, ресурси Internet
Тема №11. Атака «відмова в обслуговуванні»	
Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти перелік ресурсів, які відслідковують онлайн DOS атаки	2-3, ресурси Internet
Тема №12. SQL-ін'єкції	

Перелік питань до тем навчальної дисципліни		Література
	Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю засобів для автоматичного пошуку вразливостей, пов'язаних з SQL-ін'єкціями	2-3, ресурси Internet
	Тема №13. Соціальна інженерія	
	Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю засобів соціальної інженерії	2-3, ресурси Internet
	Тема №14. Тестування на вразливість до атак	
	Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю засобів тестування на вразливість до атак з Kali Linux	2-3, ресурси Internet
	Тема №15. Сервіси та механізми захисту мережі	
	Відпрацювати лекцію за темою. Закінчити виконання лабораторних занять. Скласти таблицю механізмів захисту мережі від збору інформації	2-3, ресурси Internet

5. Індивідуальні навчально-дослідні завдання

5.1.1. Теми рефератів

1. Порівняльний аналіз безкоштовних сервісів VPN в глобальній мережі.
2. Технології TOR мережі.
3. Технології I2P мережі.
4. Порівняльний аналіз безкоштовних персональних міжмережних екранів.
5. Порівняльний аналіз ОС тестування на вразливість до атак.

5.1.2. Теми курсових робіт

1. Аналіз та практична оцінка сервісів і програмних засобів збору інформації про веб-сайти.
2. Аналіз та практична оцінка програмних засобів збору інформації, що використовують пошуковий сервіс Google.
3. Аналіз та практична оцінка сервісів і програмних засобів збору інформації із сервісу Whois.
4. Аналіз та практична оцінка сервісів і програмних засобів збору інформації із серверів DNS.
5. Аналіз та практична оцінка сервісів і програмних засобів збору інформації про логічну і фізичну структуру віддаленої мережі.
6. Аналіз та практична оцінка сервісів і програмних засобів комплексного збору інформації в глобальній мережі.
7. Збір інформації про вузли та мережні пристрої за допомогою Shodan.
8. Аналіз та практична оцінка сервісів і програмних засобів побудови та аналізу зв'язків між частинами отриманої інформації.
9. Аналіз та практична оцінка сервісів і програмних засобів збору інформації за заголовками електронної пошти.
10. Аналіз та практична оцінка сервісів і програмних засобів OSINT.
11. Аналіз та практична оцінка сервісів і програмних засобів визначення типу і версії ОС вузла.
12. Аналіз та практична оцінка програмних засобів отримання інформації з NetBIOS.
13. Аналіз та практична оцінка програмних засобів отримання інформації з SMTP.
14. Аналіз та практична оцінка сервісів і програмних засобів пошуку вразливостей.
15. Аналіз та практична оцінка програмних засобів створення SSH-тунелю.
16. Аналіз та практична оцінка програмних засобів виявлення вторгнень.

17. Аналіз та практична оцінка програмних засобів міжмережного керування доступу.
18. Аналіз та практична оцінка програмних засобів Honeypot.
19. Аналіз та практична оцінка програмних засобів підбору гешів.
20. Аналіз та практична оцінка програмних засобів перехоплення і порівняльний аналізу мережевого трафіку.
21. Аналіз та практична оцінка програмних засобів реалізації MAC затоплення та ARP Spoofing.
22. Аналіз та практична оцінка програмних засобів атаки на DHCP сервер.
23. Аналіз та практична оцінка програмних засобів MITM атак.
24. Аналіз та практична оцінка програмних засобів вивчення та доступу до безпровідних мереж.
25. Аналіз та практична оцінка програмних засобів прискорення підбору паролів.
26. Аналіз та практична оцінка програмних засобів DoS атаки на безпровідні мережі.
27. Аналіз та практична оцінка програмних засобів створення шкідливого програмного забезпечення.
28. Аналіз та практична оцінка програмних засобів дослідження вразливостей веб-сервера.
29. Аналіз та практична оцінка програмних засобів експлуатації вразливостей операційної системи.
30. Аналіз та практична оцінка програмних засобів експлуатації вразливостей веб-сервера.
31. Аналіз та практична оцінка програмних засобів завантаження та виконання довільних файлів.
32. Аналіз та практична оцінка програмних засобів, що реалізують міжсайтову підробку запиту (Cross Site Request Forgery).
33. Аналіз та практична оцінка програмних засобів, що реалізують міжсайтовий скриптінг (Cross Site Scripting).
34. Аналіз та практична оцінка програмних засобів, що реалізують атаку "відмова в обслуговуванні".
35. Аналіз та практична оцінка програмних засобів, що реалізують SQL-ін’єкції.
36. Аналіз та практична оцінка програмних засобів соціальної інженерії.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких курсанти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних і лабораторних занять.

Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

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 IT-безпеки.
8. Архітектура безпеки ITC.
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 безпровідні мережі.
24. Шифрування та автентифікація в безпровідних мережах.
25. Атака на безпровідні мережі.
26. Засоби захисту від безпровідних атак.
27. Організація контролю доступу в ОС.
28. Руткіти 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-застосувань.
37. Види атак на веб-сервер.
38. Види атак на веб-застосування.
39. Механізми захисту веб-серверів та веб-застосувань.
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-застосувань 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.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\textit{Загальна кількість балів (перед підсумковим контролем)} = (\textit{Результат навчальних занять за семестр} + \textit{Результат самостійної роботи за семестр}) / 2) * 10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

Підсумкові бали навчальної дисципліни = ***Загальна кількість балів (перед підсумковим контролем)*** + ***Кількість балів за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

Підсумкові бали навчальної дисципліни = ***Підсумкові бали за поточний семестр*** + ***Підсумкові бали за попередній семестр*** : ***2***

Критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на практичних, лабораторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати звіт за темою самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97–100	Відмінно ("зараховано")	A	**"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")	B	**"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		C	**"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")	D	**"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		E	**"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.
41–59	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		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не**

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
			сформовані, всі виконані навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не призведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

10. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна

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 КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

Додаткова

4. Allen L., Cardwell K. Advanced Penetration Testing for Highly-Secured Environments. Second edition. — Packt Publishing, 2016.
5. 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

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/hacktivities?tab=practice