МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузь знань	**12 "Інформаційні технології"**
Спеціальність	**125 "Кібербезпека"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"Кібербезпека"**

Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та інформаційних технологій.
Протокол № 8 від 24.12.2022 р.

Розробник(и):
Лимаренко В.В., к.т.н., доц. кафедри кібербезпеки та інформаційних технологій.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

На сучасному етапі серед основних реальних загроз національній безпеці України в інформаційній сфері є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави. Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ до інформації, яка обробляється та циркулює на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також витік інформації різноманітними технічними каналами.

Саме для протидії загрозам такого роду функціонують системи технічного захисту інформації, які дозволяють вирішувати практично весь комплекс завдань з технічного захисту інформації на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах державних органів, підприємств, установ та організацій.

До складу систем протидії загрозам входять сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правова та матеріально-технічна бази і їх діяльність спрямована на забезпечення інженерно-технічних заходів забезпечення конфіденційності, цілісності та доступності інформації.

Метою навчальної дисципліни «Основи технічного захисту інформації» є отримання студентами необхідних базових знань, щодо порядку створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Основними завданнями вивчення дисципліни є систематизація інформації, щодо розроблення, впровадження та експлуатації систем технічного захисту інформації на об’єктах інформаційної діяльності.

Завданнями навчальної дисципліни є придбання навичок з проектування та створення комплексних систем захисту інформації, практичного здійснення захисту інформації на об’єктах інформаційної діяльності та виявлення можливих джерел її витоку.

Предметом навчальної дисципліни є методи та засоби забезпечення технічного захисту інформації.

Характеристика навчальної дисципліни

Курс	4
Семестр	7
Кількість кредитів ECTS	5
Форма підсумкового контролю	екзамен

Структурно-логічна схема вивчення навчальної дисципліни

Пререквізити	Постреквізити
Безпека та аудит бездротових та рухомих мереж	Комплексний тренінг
Безпека в інформаційно-комунікаційних системах	
Комплексні системи захисту інформації	

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	Виявляти небезпечні сигнали технічних засобів;

Програма навчальної дисципліни

Змістовий модуль 1. Технічні канали витоку інформації

Тема 1. Інформаційна безпека як складова національної безпеки. Основні поняття та категорії. Нормативно-правове забезпечення інформаційної безпеки

Тема 2. Технічний канал витоку інформації. Організаційно-технічні заходи щодо технічного захисту інформації на об’єкті

Тема 3. Виток акустичної інформації – виявлення та захист

Змістовий модуль 2. Технічні засоби забезпечення безпеки даних в комп'ютерних системах та мережах

Тема 4. Загрози безпеці даних в комп'ютерних системах та мережах

Тема 5. Захист пристроїв, що працюють під управлінням ОС Windows

Тема 6. Захист пристроїв, що працюють під управлінням ОС Linux

Тема 7. Забезпечення безпеки даних в комп'ютерних мережах

Тема 8. Забезпечення безпеки даних мережевих пристроїв

Тема 9. Загроза безпеки даних від дій хакерів

Тема 10. Атаки на базові функції мереж

Тема 11. Засоби захисту безпеки комп'ютерних мереж

Тема 12. Захист кінцевих пристроїв

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці «Рейтинг-план навчальної дисципліни».

Методи навчання та викладання

Викладання дисципліни передбачає залучення пояснювально-ілюстративного, репродуктивного, дослідницького методів, а також методів проблемного навчання. Так під час проведення лекційних занять викладач надає здобувачам певний обсяг теоретичного матеріалу (теми 1-12), приклади застосування різноманітних технологій та засобів технічного захисту інформації (теми 1-12), з наданням пояснень у графічному вигляді (схеми, таблиці, презентації) та за допомогою прикладів (теми 1-12). На лабораторних заняттях здобувачі мають змогу отримати практичні навички пошуку вирішення проблем на підставі вихідних даних, сформульованих за тематикою заняття (роботи 1-6). Вдосконалення практичних навичок відбувається під час виконання самостійної роботи (теми 1-12).

Наведені методи навчання спрямовані на формування у здобувачів здатності розв'язання складних комплексних задач з технічного захисту інформації.

Порядок оцінювання результатів навчання

ХНЕУ ім. С. Кузнеця використовує накопичувальну (100-бальну) систему оцінювання. Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи.

Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що надає студенту допуск до екзамену, – 40 балів);

2) підсумковий/семестровий контроль, що проводиться у формі екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

– вміння розуміти та пояснювати поняття, можливості та проблеми сучасних систем технічного захисту інформації;

– вміння розробляти та моделювати комплексну структуру систем технічного захисту інформації з урахуванням особливостей об'єктів захисту;

– вміння діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

– вміння вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою;

– вміння здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

– вміння аналізувати структуру та технічний склад комп'ютерних систем різного призначення з ціллю виявлення можливих технічних каналів витоку інформації.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: в технологічній карті бали на цей вид робіт не виділені.

Лабораторні заняття: максимальна кількість балів становить 60 (виконання та захист лабораторних робіт – 60), а мінімальна – 40.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями, в технологічній карті бали на цей вид робіт не виділені.

Підсумковий контроль: проводиться у вигляді екзамену, максимальна кількість балів становить 40. Екзаменаційний білет складається з двох теоретичних питань та одного практичного завдання. Максимальна кількість балів за кожне теоретичне питання складає 10, а за вирішення практичного завдання – 20. Мінімальна умова допуску до екзамену – отримання мінімального балу за лабораторні роботи (40). В разі невиконання плану лабораторних робіт студент до екзамену вважається не допущеним.

Загальна сума балів підсумкової/семестрової перевірки успішності складається з балів за лекційні заняття, лабораторні роботи і екзамен. Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням 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.

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання	Форми оцінювання	Max бал
1	2	3	4
Змістовий модуль 1. Технічні канали витоку інформації			
ТЕМА 1.	***Аудиторна робота***		
	Лекція 1. Інформаційна безпека як складова національної безпеки. Основні поняття та категорії. Нормативно-правове забезпечення інформаційної безпеки	Активна робота	
	Лабораторна робота 1. Ч.1. Моделювання об'єкта захисту	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 2.	***Аудиторна робота***		
	Лекція 2. Технічний канал витоку інформації. Організаційно-технічні заходи щодо технічного захисту інформації на об’єкті	Активна робота	
	Лабораторна робота 1. Ч.2. Моделювання об'єкта захисту	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
	Аудиторна робота		

ТЕМА 3.	Лекція 3. Виток акустичної інформації – виявлення та захист	Активна робота	
	Лабораторна робота 2. Ч.1 Засоби перехоплення інформації в акустичному діапазоні хвиль	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
Змістовий модуль 2. Технічні засоби забезпечення безпеки даних в комп'ютерних системах та мережах			
ТЕМА 4.	***Аудиторна робота***		
	Лекція 4. Загрози безпеці даних в комп'ютерних системах та мережах	Активна робота	
	Лабораторна робота 2. Ч.2 Засоби перехоплення інформації в акустичному діапазоні хвиль	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 5.	***Аудиторна робота***		
	Лекція 5. Захист пристроїв, що працюють під управлінням ОС Windows	Активна робота	
	Лабораторна робота 3. Ч.1. Навігація у файловій системі Linux і настроювання повноважень	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 6.	***Аудиторна робота***		
	Лекція 6. Захист пристроїв, що працюють під управлінням ОС Linux	Активна робота	
	Лабораторна робота 3. Ч.2. Навігація у файловій системі Linux і настроювання повноважень	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 7.	***Аудиторна робота***		
	Лекція 7. Забезпечення безпеки даних в комп'ютерних мережах	Активна робота	
	Лабораторна робота №4. Ч.1. Вивчення перехоплених пакетів TCP і UDP за допомогою програми Wireshark	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 8.	***Аудиторна робота***		
	Лекція 8. Забезпечення безпеки даних мережевих пристроїв	Активна робота	

	Лабораторна робота №4. Ч.2. Вивчення перехоплених пакетів TCP і UDP за допомогою програми Wireshark	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 9.	***Аудиторна робота***		
	Лекція 9. Загроза безпеки даних від дій хакерів	Активна робота	
	Лабораторна робота №5. Ч.1. Атака на базу даних mySQL	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 10.	***Аудиторна робота***		
	Лекція 10. Атаки на базові функції мереж	Активна робота	
	Лабораторна робота №5. Ч.2. Атака на базу даних mySQL	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 11.	***Аудиторна робота***		
	Лекція 11. Засоби захисту безпеки комп'ютерних мереж	Активна робота	
	Лабораторна робота №6. Ч.1. Шифрування і розшифрування даних за допомогою OpenSSL	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
ТЕМА 12.	***Аудиторна робота***		
	Лекція 12. Захист кінцевих пристроїв	Активна робота	
	Лабораторна робота №6. Ч.2. Шифрування і розшифрування даних за допомогою OpenSSL	Виконання лабораторної роботи	5
	Самостійна робота		
	Вивчення лекційного матеріалу, підготовка до лабораторного заняття		
	Іспит		40

Рекомендована література

Основна

1. Хорошко В.А. Методи і засоби захисту інформації / В.А. Хорошко, А.А. Чекатков. – К.: Юниор, 2019. – 504 с.

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 16.12.2020 р. // https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

3. Коженевський С.Р. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2019. – 365 с.

4. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – К. : Новий світ-2000, 2021 р. – 678 с.

5. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO / Т. І. Коробейнікова, С. М. Захарченко. – Львів, : Львівська політехніка, 2021 р. – 232 с.

6. Василь Лизанчук. Інформаційна безпека України: теорія і практика / Василь Лизанчук. – Львів, : ЛНУ, 2021 р. – 728 с.

Додаткова

1. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2020.

2. Рибальский О.В. Основи інформаційної безпеки та технічного захисту інформації / Рибальский О.В. Хахановський В.Г., Кудінов В.А. – К.: Вид. Національної академії внутріш. справ, 2022. – 104 с.

Інформаційні ресурси в Інтернеті

1. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Основи технічного захисту інформації» https://pns.hneu.edu.ua/course/view.php?id=8958.

2. Державна служба спеціального зв’язку та захисту інформації України // https://cip.gov.ua/ua/statics/zakhist-informaciyi

3. Захист інформації в системах електронного урядування // https://old.suitt.edu.ua/wp-content/uploads/2018/05/Part_013_Feb_2018.pdf

4. Системи захисту інформації у фінансових установах // https://buklib.net/books/28521