Силабус курсу

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь вищої освіти – бакалавр
Рік навчання: 4**,**
Семестр: 7
Кількість кредитів: 5**,**
Мова викладання: українська

Керівник курсу

ПІП	Сергій Кулина
Контактна інформація	sersks@wunu.edu.ua

Опис дисципліни

Курс «Технічні засоби захисту інформації» орієнтований на формування компетентностей та умінь щодо технічного захисту інформації для їх використання в сучасних комп'ютерних системах, а також знаннями щодо проявлення різних технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування різних технічних заходів та засобів, які спрямовані на захист інформації на об'єктах інформаційної діяльності.

Вивчення курсу вимагає цілеспрямованої роботи над вивченням спеціалізованої літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань. Мета курсу полягає в отриманні студентами необхідних знань щодо проявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності.

Структура курсу

Години лек / лаб	Тема	Результати навчання	Завдання
2/-	Види, джерела та носії інформації, що підлягають захисту	Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій	Поточне опитування
2/4	Небезпечні сигнали та їх джерела	Виявляти небезпечні сигнали технічних засобів. Розуміти основні поняття та виявляти небезпечні сигнали технічних засобів	Поточне опитування
4/2	Технічна розвідка	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно телекомунікаційних систем	Поточне опитування
4/4	Концепція і методи технічного захисту	Володіти навичками застосування методів комплексного захисту, знати основні напрямки	Поточне

	інформації	інженерно-технічного захисту	опитування
4/4	Технічні канали витоку інформації	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації	Поточне опитування
2/2	Електричні канали витоку інформації	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації	Поточне опитування
4/4	Радіоелектронні канали витоку інформації	Знати особливості, структуру та види витоку інформації через радіоелектронні канали. Класифікувати типи перешкод.	Поточне опитування
4/4	Акустичні канали витоку інформації	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.	Поточне опитування
4/4	Технічні канали витоку інформації на основі закладних пристроїв	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах	Поточне опитування
4/4	Методи та засоби захисту від спостереження та підслуховування	Розуміти поняття енергетичне приховування, звукоізоляція та звукопоглинання. Знати методи та засоби виявлення випромінювання та не випромінюючих закладних пристроїв	Поточне опитування
4/4	Засоби запобігання витоку інформації через побічні електромагнітні випромінювання	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки	Поточне опитування
4/4	Методи і засоби приховування інформації в каналах зв’язку	Знати методи приховування мовної інформації в каналах зв’язку, засоби контролю телефонних ліній та перехоплення повідомлень в GSM каналах	Поточне опитування
4/4	Методи і засоби технічної охорони об’єктів. системи сигналізації та відео спостереження	Знати складові та властивості систем телевізійного спостереження, засобів телевізійної охорони. Основні характеристики засобів запису та реєстрації зображення	Поточне опитування

Рекомендовані джерела інформації

1. Яцків, В. В., Кулина, С. В. (2023). Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека». – Тернопіль 2023. – 88 с.
2. Кулина, С. В. (2023). Виявлення та виправлення помилок у захищених системах зберігання даних на основі обчислення проекцій числа. *Informatics and Mathematical Methods in Simulation*. Vol. 12, 2022, No. 4, pp. 337-345.
3. Кулина, С. В. (2023). Система розподіленого захищеного зберігання даних. *Вісник Львівського державного університету безпеки життєдіяльності*, № 27, 2023. С.48-59.
4. Аль-Амморі, А. (2024). *Елементи теорії надійності та інформаційної безпеки комп’ютеризованих систем*: навч. посіб. Київ: Ліра-К. 282 с.

5. Богуш, В. М., Бровко, В. Д., Кобус, О. С., & Козюра, В. Д. (2022). *Технічний захист інформації*. Ч. 1: *Основи технічного захисту інформації*: навч. посіб. Київ: Ліра-К. 286 с.
6. Богуш, В. М., Богуш, В. В., Бровко, В. Д., & Настрадін, В. П. (2020). *Основи кіберпростору, кібербезпеки та кіберзахисту*: навч. посіб. Київ: Ліра-К. 554 с.
7. Богуш, В. М., Бровко, В. Д., Кобус, О. С., & Козюра, В. Д. (2022). *Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення*. Київ: Ліра. 286 с.
8. Сальник, В. В., Гуж, О. А., Закусіло, В. С., Сальник, С. В., & Бєляєв, П. В. (2021). Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах. *Збірник наукових праць Харківського національного університету Повітряних Сил*, (4 (70)), 77-82.
9. Остапов, С. Е., Євсеєв, С. П., & Король, О. Г. (2023). *Технології захисту інформації*: навч. посіб. Львів: Новий світ-2000. 678 с.
10. Гулак, Г. М. (2020). *Методологія захисту інформації. Аспекти кібербезпеки*: підручник. Київ: НА СБ України. 256 с.
11. Євсеєв, С. П., Заковоротний, О. Ю., Мілов, О. В., Кучук, Г. А., Галуза, О. А., Коваль, М. В., Войтко, О. В., & Грищук, Р. В. (2024). *Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури*: монографія. Харків: Новий Світ-2000. 300 с.
12. Лаптєв, О. А., Савченко, В. А., & Шуклін, Г. В. (2020). *Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності*: навч. посіб. Київ: ДУТ. 126 с.
13. Полторак, В. П. (2020). *Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах*: навч. посіб. Київ: КПІ ім. Ігоря Сікорського. 78 с.
14. CCTA Risk Analysis and Management Method. (н.д.). URL: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysismanagement-tool-cramm/103133.

Політика оцінювання

Політика щодо запізнення та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування: За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Цифрова криміналістика» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-8.	Підсумкове модульне тестування за темами № 1-9.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 9-13.	Підсумкове модульне тестування за темами № 10-13.	Визначається як середнє арифметичне з оцінок за завдання тренінгу (не менше двох).	Визначається як оцінка за наскрізне завдання самостійної роботи.	1. Теоретичні питання: 2 Питання по 20 балів. 2. 15 тестів по 4 бали.

Виконання лабораторних робіт:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі кроки в рамках лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами, що відносяться до теми дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання лабораторної роботи, проте в процесі виконання допустив кілька дрібних помилок, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання лабораторної роботи, але з суттєвими помилками, наприклад, не з першого разу чи не до кінця. Розуміння поставлених у лабораторній роботі завдань є поверхневим та неповним.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з програмним забезпеченням.

Підсумкове модульне тестування - вид контролю, при якому засвоєний здобувачем освіти теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 40 запитань кожна правильна відповідь дає 2,5 бали, максимум 100 балів.

Тренінг:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат, в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у тренінгу завдань є поверхневим.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував достатній рівень навичок роботи з апаратним та програмним забезпеченням.

Самостійна робота:

90–100 балів (Відмінно) - доповідь охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Дослідження містить не лише опис, але й аналіз, порівняння різних методів та засобів, висновки обґрунтовані. У процесі написання звіту використані сучасні джерела інформації, що свідчить про обізнаність здобувача освіти з напрямом дослідження. Здобувач освіти вільно володіє матеріалом, доповідає впевнено та відповідає на всі запитання.

75–89 балів (Добре) - доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими; використані джерела інформації є релевантними, але не найновішими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

60–74 балів (Задовільно) - доповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач не завжди впевнено відповідає на запитання, а сам виступ може бути нечітким.

1–59 балів (Незадовільно) - зміст доповіді не відповідає темі або є компіляцією застарілих даних. Робота є прямим копіюванням без самостійного опрацювання.

Екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу з дисципліни «Технічні засоби захисту інформації». Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитання, за кожне з яких можна отримати від 0 до 20 балів, що в підсумку дає максимально 40 балів. За відповідь на питання здобувач освіти отримує 11–20 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–10 балів – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить 15 тестових завдань. За кожну правильну відповідь тестування здобувач освіти отримує 4 бали, максимум 60 балів.

Шкала оцінювання

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов’язковим повторним курсом)