Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем
Кафедра інформаційно-комунікаційних технологій та систем

ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

СИЛАБУС

для технічних спеціальностей КПІ ім. Ігоря Сікорського

РЕКВІЗИТИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Рівень вищої освіти	перший (бакалаврський)
Галузь знань	для галузі знань 17
Спеціальність	спеціальність 172
Освітня програма	освітня програма Інформаційно-комунікаційні технології
Статус дисципліни	обов'язкова
Форма навчання	очна (денна)
Рік підготовки, семестр	рік четвертий, семестр 2 відповідно до додатку 3 наказу № НОН/18/2021 від 01.02.2021 Про організацію та планування освітнього процесу на 2021-2022 навчальний рік
Обсяг дисципліни	4 кредити ЄКТС (120 годин), з них лекції 27 годин, практичні заняття 18 годин, самостійна робота 60 годин
Семестровий контроль / контрольні заходи	Модульна контрольна робота Іспит
Розклад занять	Згідно з розкладом
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектори та викладачі лабораторних занять: кафедри https://ikts-its.kpi.ua/vykladachi-kafedry/
Розміщення курсу	Визначається лектором відповідної частини курсу та доводиться до відома студентів на першому занятті

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

1.1. Опис навчальної дисципліни

Навчальна дисципліна складається з трьох розділів:

- Розділ 1. «Основи захисту інформації».
- Розділ 2. «Комплексні системи захисту ТКС від загроз».
- Розділ 3. «Нормативно-правові засади захисту інформації в ТКС».

1.2. Мета навчальної дисципліни

Метою навчальної дисципліни є підготовка фахівця, який має базові компетенції в області сучасних технологій використання методів захисту інформації та програмних засобів і прикладних програм для перевірки рівня захисту інформаційних систем обміну даними.

Метою навчальної дисципліни є формування у студентів **компетентностей**:

- використовувати засоби розмежування доступу;
- виявляти атаки на телекомунікаційні системи;
- застосовувати засоби цифрового підпису;
- виконувати мережеве екранування;

- застосовувати криптографічний захист інформації.

1.3. Предмет вивчення дисципліни

Предмет навчальної дисципліни – сукупність апаратних та програмних рішень для аналізу захищеності мережі, виявлення вторгнень та впровадження заходів для безпечного обміну інформацією в телекомунікаційних системах.

1.4. Результати навчання

- Використовувати засоби криптографічного захисту інформації.
- Застосовувати засоби розмежування доступу.
- Використовувати засоби виявлення атак.
- Використовувати засоби цифрового підпису.
- Впроваджувати засоби мережевого екранування.

2. Пререквізити та постреквізити дисципліни

Перелік дисциплін або знань та умінь, володіння якими необхідні здобувачу вищої освіти для успішного засвоєння дисципліни	Перелік дисциплін, які базуються на результатах навчання з даної дисципліни
Дисципліна вивчається на основі предметів цифрових технологій та програмування: «Інформатика», «Цифрове оброблення сигналів», «Схемотехніка»	• Наукова робота за темою бакалаврської роботи • Практика

3. Зміст навчальної дисципліни

Розділ 1. Основи захисту інформації
Тема 1. Шифрування і хешування.
Тема 2. Служба Secure Shell.
Розділ 2. Комплексні системи захисту ТКС від загроз
Тема 3. Безпека фізичного і канального рівнів, міжмережеві екрани.
Тема 4. Виявлення мережевих атак.
Тема 5. Нові тенденції в технологіях захисту.
Розділ 3. Нормативно-правові засади захисту інформації в ТКС
Тема 6. Національний стандарт шифрування ДСТУ 7624:2014.
Тема 7. Стандартизація у галузі захисту інформації.

4. Навчальні матеріали та ресурси

Базова література:

1. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник, 2018. / [За редакцією О.В.Лісового та ін.]. -К., 2018, - 105 с. (Електронна версія http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne)
2. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 200’. — 352 с.
3. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

Додаткова література:

1. Akashdeep Bhardwaj, Varun Sapra. Security Incidents & Response Against Cyber Attacks. Springer, 2021, - 250 p.
2. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
3. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Електронний ресурс] : підручник / М. В. Грайворонський, О. М. Новіков. – Київ : Видавнича група BHV, 2009. – 698 с.

Інформаційні ресурси Інтернету:

1. Персональний сайт викладача: - http://isearch.kiev.ua/uk/searchpractice/internetsecurity

2. Сайт дистанційного навчання на платформі Moodle Академії Mikrotik: - http://iot.kpi.ua/lms/
3. Платформа дистанційного навчання «Сікорський»: - https://www.sikorsky-distance.org/

НАВЧАЛЬНИЙ КОНТЕНТ

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1. Розподіл занять за темами

Розділ 1. Основи захисту інформації

Тема 1. *Лекція 1*. Вступ в безпеку комп'ютерних мереж.
- Практичне заняття 1. Методи отримання інформації.

Лекція 2. Шифрування і хешування для захисту інформації.
- Практичне заняття 2. Дослідження вбудованих в ОС Windows методів шифрування.
- Практичне заняття 3. Використання Wireshark для аналізу трафіка.
- Практичне заняття 4. Захоплення і розшифровка бездротового трафіку.

Тема 2. *Лекція 3*. Служба Secure Shell.
- Практичне заняття 5. Налаштування SSH.

Розділ 2. Комплексні системи захисту ТКС від загроз

Тема 3. *Лекція 4*. Безпека фізичного і канального рівнів. Мережеві аналізатори і «сніфери»
- Практичне заняття 6. Інвентаризація мережевих ресурсів з використанням утиліти `nmap`.

Лекція 5. Фільтрація трафіка. Міжмережеві екрани
- Практичне заняття 7. Налаштування файрвола Comodo.

Лекція 6. Віртуальні приватні мережі.
- Практичне заняття 8. Побудова виділеного VPN-сервера.

Лекція 7. Аналіз захищеності мережевих ресурсів.

Тема 4. *Лекція 8*. Виявлення мережевих атак.
- Практичне заняття 9. Встановлення та налаштування IDS на Snort.

Тема 5. *Лекція 9*. Використання машинного навчання для підвищення безпеки комп'ютерних мереж.
Лекція 10. Безпека в IoT: архітектура системи безпеки.

Розділ 3. Нормативно-правові засади захисту інформації в ТКС

Тема 6. *Лекція 11*. Симетричний блоковий шифр «Калина». Національний стандарт ДСТУ 7624:2014.
Тема 7. Лекція 12. Нормативно-правові засади захисту інформації в ТКС.
Лекція 13. Стандартизація в галузі захисту інформації в ТКС.

Модульна контрольна робота (тести при дистанційному навчанні):
1. За темами 1, 3-6
Підготовка до іспиту
Іспит

5.2. Методика опанування

Лекції

Розділ 1. Основи захисту інформації

Лекція 1. Вступ в безпеку комп'ютерних мереж
Зміст лекції:
1. Типова IP-мережа організації.
2. Рівні інформаційної інфраструктури корпоративної мережі.
3. Концепція глибокоешелонованого захисту**.**
4. Термінологія. Загрози, вразливості і атаки**.**

5. Джерела виникнення вразливостей.
6. Класифікація вразливостей за ступенем (рівнем) ризику.

Лекція 2. Шифрування і хешування для захисту інформації

Зміст лекції:

1. Симетричне і асиметричне шифрування, їх переваги і недоліки.
2. Хешування паролів.
3. Методи злому паролів, демаскуючі фактори спроб компрометації паролів.
4. Особливості системи шифрування, вбудованої в ОС Windows.
5. Базова структура системи шифрування, впровадженої в корпорації.

Лекція 3. Служба Secure Shell

Зміст лекції:

1. Стандарти та програмні реалізації протоколу SSH (*Secure SHell* — «безпечна оболонка»).
2. Поняття SSH-сервера і SSH-клієнта.
3. Команди SSH.
4. SSH-тунель.
5. Вразливості протоколу SSH.

Розділ 2. Комплексні системи захисту ТКС від загроз

Лекція 4. Безпека фізичного і канального рівнів. Мережеві аналізатори і «сніфери»

Зміст лекції:

1. MAC-адреса і розмежування доступу**.**
2. Зміна MAC-адреси**.**
3. Мережеві аналізатори («сніфери»).
4. Захист від «сніферів».
5. Виявлення сніферів.

Лекція 5. Фільтрація трафіка. Міжмережеві екрани

Зміст лекції:

1. Захист периметра.
2. Базові відомості про міжмережеві екрани.
3. Технологія «stateful inspection».
4. Шлюзи рівня з'єднання.
5. Шлюзи прикладного рівня.
6. Системи аналізу вмісту.
7. Пакетний фільтр на базі Linux (iptables).
8. Приклад конфігурування iptables.

Лекція 6. Віртуальні приватні мережі

Зміст лекції:

1. Різновиди VPN-технологій.
2. Реалізація VPN-технологій.
3. Схеми використання технологій VPN.
4. Короткі відомості про IPsec.
5. Протокол Authentication Header (AH).
6. Протокол Encapsulated Security Payload (ESP).
7. Алгоритми, рекомендовані RFC 4305.
8. Протокол IKE.
9. Протокол L2TP.
10. Протокол PPTP.

Лекція 7. Аналіз захищеності мережевих ресурсів

Зміст лекції:

1. Керування вразливостями.
2. Архітектура систем керування вразливостями.
3. Мережеві агенти сканування.
4. Ідентифікація вразливостей.
5. Статистика аналізу захищеності.
6. Висновки та рекомендації інструментального аналізу захищеності.

Лекція 8. Виявлення мережевих атак

Зміст лекції:

1. Необхідність технології виявлення атак.
2. Архітектура систем виявлення атак**.**
3. Джерела даних**.**
4. Технологія виявлення**.**
5. Механізми реагування.
6. Система виявлення атак `Snort`.

Лекція 9. Використання машинного навчання для підвищення безпеки комп'ютерних мереж

Зміст лекції:

1. Технології машинного навчання (МН) і їх застосування в телекомунікаціях.
2. Алгоритми МН для виявлення ознак втручання в систему.
3. Особливості алгоритмів МН для фільтрації спаму.
4. Використання нейромережі для виявлення атак.

Лекція 10. Безпека в IoT: архітектура системи безпеки

Зміст лекції:

1. Моделювання ризиків в основі безпеки**.**
2. Ключові етапи та кроки моделювання.
3. Безпека в середовищі IoT.
4. Зони пристрою, польового і хмарного шлюзів, служб.
5. Порівняння інформаційних і спеціалізованих пристроїв.
6. Управління пристроєм і взаємодія з даними на пристрої.
7. Еталонна архітектура Azure IoT: моделювання ризиків.

Розділ 3. Нормативно-правові засади захисту інформації в ТКС

Лекція 11. Симетричний блоковий шифр «Калина». Національний стандарт ДСТУ 7624:2014

Зміст лекції:

1. Стандартні режими роботи.
2. Нові режими роботи: призначення та властивості.
3. Позначення та приклади для перевірки.
4. Перспективи розвитку блокових перетворень в умовах постійного вдосконалення криптоаналітичних комплексів.

Лекція 12. Нормативно-правові засади захисту інформації в ТКС

Зміст лекції:

1. Етапи створення системи захисту в ТКС.
2. Базові документи правових засад систем захисту інформації в ТКС .

Лекція 13. Стандартизація в галузі захисту інформації в ТКС

Зміст лекції:

1. Офіційні документи для стандартизації рішень в галузі захисту інформації.
2. Послідовність впровадження та сертифікації систем захисту інформації в ТКС.

Практичні заняття

Розділ 1. Основи захисту інформації

Практичне заняття 1. Методи отримання інформації

Теоретична частина

Використовується матеріал Лекції 1 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Ознайомлення з основними елементами на платі мікрокомп'ютера Raspberry Pi. Організація підключення до мікрокомп'ютера. Виконання основних команд ОС Raspbery на ядрі Linux (список надається).

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Практична частина для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 2. Дослідження вбудованих в ОС Windows методів шифрування

Теоретична частина

Використовується матеріал Лекції 1 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Організація віддаленого доступу з Інтернету до мікрокомп'ютера. Налаштування підключення Rasberry Pi до однієї, або кількох мереж Wi-Fi.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 3. Використання Wireshark для аналізу трафіка

Теоретична частина

Використовується матеріал Лекції 2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Організація двох стороннього обміну файлами між ПК і Raspberry Pi: створення файлів, завантаження та встановлення необхідного програмного забезпечення, пересилання файлів з використанням різних програмних інструментів.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 4. Захоплення і розшифровка бездротового трафіку

Теоретична частина

Використовується матеріал Лекції 2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Налаштування безпечного підключення до Raspberry Pi через протокол SSH в локальній мережі: запуск VNC, завантаження та встановлення клієнта, запуск клієнта, в тому числі, на смартфоні. Автоматизація та запуск VNC при завантаженні.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 5. Налаштування SSH

Теоретична частина

Використовується матеріал Лекції 3 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії
Встановлення Apache і PHP. Встановлення MySQL. Перевірка веб-сервера. Зміна веб-сторінки за замовчуванням. Встановлення Joomla на Raspberry Pi. Налаштування Joomla з веб-браузера
Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.
Завдання для самостійної роботи
Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Розділ 2. Комплексні системи захисту ТКС від загроз

Практичне заняття 6. Інвентаризація мережевих ресурсів з використанням утиліти `nmap`
Теоретична частина
Використовується матеріал Лекції 3 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.
Практична частина під час роботи в аудиторії
Підключення камери. Використання raspistill. Отримання фото для різних параметрів зйомки. Написання Bash-сценарій для автоматизації звереження фотографій. Використання команди raspivid для збереження відеопотоку. Використання Time-lapse для отримання відеоряду з окремих кадрів.
Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.
Завдання для самостійної роботи
Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 7. Налаштування файрвола Comodo
Теоретична частина
Використовується матеріал Лекції 4 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.
Практична частина під час роботи в аудиторії
Встановлення бібліотеки для роботи з GPIO. Нумерація виводів GPIO та їх призначення. Перевірка роботи GPIO Raspberry Pi в стилі Arduino. Збирання схеми на монтажній платі для перевірки реалізованого програмного забезпечення.
Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.
Завдання для самостійної роботи
Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 8. Побудова виділеного VPN-сервера
Теоретична частина
Використовується матеріал Лекції 4 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.
Практична частина під час роботи в аудиторії
Завантаження та встановлення WebIOPi - фреймворк Інтернету речей для Raspberry Pi. Запуск WebIOPi в різних режимах. Дослідження доступу WebIOPi через локальну мережу.
Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.
Завдання для самостійної роботи
Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Практичне заняття 9. Встановлення та налаштування IDS на Snort
Теоретична частина
Використовується матеріал Лекції 4 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.
Практична частина під час роботи в аудиторії
Виконання окремих команд в середовищі пакету Mathematica з використанням мови Wolfram. Запуск Mathematica, програмування в Mathematica. Виконання обчислень через командний рядок Wolfram.
Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.
Завдання для самостійної роботи
Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

6. Самостійна робота здобувачів вищої освіти

До самостійної роботи студентів включається підготовка до аудиторних занять шляхом опанування матеріалів лекцій, вивчення базової, додаткової літератури, виконання практичних робіт. Всі матеріали для СРС розміщуються на платформі дистанційного навчання Moodle (https://iot.kpi.ua/lms) та копіюються на платформу дистанційного навчання «Сікорський» (https://do.ipo.kpi.ua/course/index.php?categoryid=29).

Розділ 1. Основи захисту інформації

Тема 1. Шифрування і хешування
СРС до Практичних занять 1-4.

Тема 2. Служба Secure Shell
СРС до Практичного заняття 5.

Розділ 2. Комплексні системи захисту ТКС від загроз

Тема 3. Безпека фізичного і канального рівнів, міжмережеві екрани
СРС до Практичних занять 6-8.

Тема 4. Виявлення мережевих атак
СРС до Практичного заняття 9.

Тема 5. Нові тенденції в технологіях захисту
СРС до Лекцій 9-10.

Розділ 3. Нормативно-правові засади захисту інформації в ТКС

Тема 6. Національний стандарт шифрування ДСТУ 7624:2014
СРС до Лекцій 11-12.

Тема 7. Стандартизація у галузі захисту інформації
СРС до Лекції 13.

Підготовка до іспиту.

ПОЛІТИКА ТА КОНТРОЛЬ

7. Політика навчальної дисципліни (освітнього компонента)

7.1. Форми роботи

Лекції проводяться з використанням наочних засобів представлення матеріалу та з використанням методичних матеріалів, доступ до яких наявний у здобувачів вищої освіти. Студенти отримують всі матеріали через навчальну платформу Moodle, e-mail, кампус чи telegram-групу.

Здобувачі вищої освіти залучаються до обговорення лекційного матеріалу та задають питання, щодо його сутності.

При виконанні практичних робіт застосовуються форми індивідуальної та колективної роботи (командна робота, парна робота) для реалізації завдань викладача на набуття навичок самостійної практичної роботи.

Під час вивчення курсу застосовуються стратегії активного і колективного навчання, які визначаються наступними методами і технологіями:

1. методи проблемного навчання (проблемний виклад, частково-пошуковий (евристична бесіда) і дослідницький метод);
2. особистісно-орієнтовані (розвиваючі) технології, засновані на активних формах і методах навчання («мозковий штурм», «аналіз ситуацій» тощо);
3. інформаційно-комунікаційні технології, що забезпечують проблемно-дослідницький характер процесу навчання та активізацію самостійної роботи здобувачів вищої освіти (електронні презентації, застосування на основі комп'ютерних і мультимедійних засобів практичних завдань (тести), доповнення традиційних навчальних занять засобами взаємодії на основі мережевих комунікаційних можливостей (програмні засоби, мобільні додатки тощо).

7.2. Правила відвідування занять

Заняття можуть проводитись в навчальних аудиторіях згідно розкладу. Також заняття можуть проводитись дистанційно в асинхронному режимі з використанням навчальної платформи Moodle з однозначною ідентифікацією здобувача вищої освіти. Проведення занять онлайн повинне бути передбачене відповідним наказом по КПІ ім. Ігоря Сікорського.

За наявності поважних причин здобувач вищої освіти повинен завчасно (за 1 день) повідомити викладача про причини можливого пропуску контрольного заходу. Всі контрольні заходи (тести) в дистанційному режимі проводяться синхронно (одночасно для всіх студентів).

Якщо завчасно повідомити не вдалось, здобувач вищої освіти протягом одного тижня має зв'язатись з викладачем для погодження форми і порядку усунення заборгованості.

Якщо аудиторне заняття випадає на неробочий день (святковий, пам'ятний тощо), то матеріал такого заняття частково переходить в категорію «Самостійна робота здобувачів вищої освіти», а частково додається до наступного заняття.

7.3. Правила призначення заохочувальних та штрафних балів

Заохочувальні бали:

+10 балів – студенту автору статті (доповіді на конференції) за тематикою курсу (тільки за умови подання комплекту матеріалів).

Сума всіх заохочувальних балів не може перевищувати 10 балів.

Штрафні бали:

-1 бал за затримку завантаження протоколу ЛР (понад 5 днів) та відсутність без поважних причин на практичному занятті.

8. Політика університету

8.1. Політика щодо академічної доброчесності

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

8.2. Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

ОЦІНЮВАННЯ ТА КОНТРОЛЬНІ ЗАХОДИ

9. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

9.1. Види контролю

Вид контролю	*Спосіб контролю*
Поточний контроль	Частина 1. Перевірка підготовки до практичних занять (експрес-опитування, тестування) Частина 2. Перевірка виконання практичних робіт відповідно до розкладу занять, модульні контрольні роботи
Календарний контроль	Проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу
Семестровий контроль	Іспит

9.2. Рейтингова система оцінювання результатів навчання

Головна частина рейтингу студента формується через активну участь у практичних занять та отримання результатів модульної контрольної роботи (тестів).

Модульну контрольну роботу та іспит проводить лектор - викладач кафедри інформаційно-комунікаційних технологій та систем**.**

1) Поточний контроль

Проводяться експрес-опитування за темою заняття, виконання тестових завдань.

Рейтинг студента складається з балів, що отримуються за експрес-опитування за темою заняття, обговорення правових кейсів, вирішення практичних завдань, доповнення відповідей інших студентів у процесі дискусії на практичних заняттях, виконання тестових завдань онлайн. У випадку відсутності студента на практичному занятті, необхідно відпрацювати пропущене заняття. Виконання всіх практичних занять є умовою отримання позитивної оцінки за результатами навчання.

1. Практичні заняття
   Ваговий бал – 4
   За виконання практичного завдання:
   – завдання виконано повністю і самостійно 4;
   – завдання виконано не повністю або за допомогою викладача 1–3;
   – завдання практично не виконане 0.
   Максимальна кількість балів за практичні заняття: $R_{ПР} = 4 * 9 = 36$ балів.
2. Модульний контроль (МКР) – у вигляді чотирьох тестів.
   Правильно і повністю виконані всі завдання тесту – 8 бали, тобто, тобто максимальна кількість балів за МКР дорівнює: $R_{\text{МКР}} = 8 * 4 = 32$ бали

Штрафні та заохочувальні бали за (сума як штрафних, так і заохочувальних балів не має перевищувати $0{,}1r_C$ (4 бали):

- відсутність на практичному занятті без поважних причин –1
- участь у модернізації, супроводженні та адмініструванні дисципліни, виконання завдань з удосконалення методичних та дидактичних матеріалів з дисципліни +1…+2

Загальний рейтинговий бал дисципліни (максимум 100 балів):

$$R_Σ = R_I + R_{ПР} + R_{МКР},$$

де R_I – рейтинговий бал за підсумкову контрольну роботу (іспит)з дисципліни (від 0 до 32 балів);
$R_{ПР}$ – рейтингові бали за виконання практичних робіт 1-9;
$R_{МКР}$ – рейтингові бали за модульну контрольну роботу (тести)

Остаточний рейтинг не може перевищувати 100 балів.

2) Календарний контроль

Здійснюється двічі на семестр як моніторинг поточного стану виконання вимог силабусу

Критерій	*Перший*	*Другий*
Термін	*8-й тиждень*	*14-й тиждень*
Умови отримання позитивного результату	якщо поточний рейтинговий бал складає не менше 50% від максимально можливого балу на момент календарного контролю	якщо поточний рейтинговий бал складає не менше 50% від максимально можливого балу на момент календарного контролю

3) Залікова контрольна робота

Максимальна рейтингова оцінка без врахування підсумкової контрольної роботи (іспиту) складає 70 балів.

Якщо здобувача вищої освіти не задовольняє набрана кількість балів, то результати рейтингової оцінки не скасовуються, а здобувач вищої освіти пише контрольну роботу (здає іспит) з дисципліни, бали якої додаються до отриманих раніше.

Підсумкова контрольна робота являє собою тест, який може бути оцінений від 0 до 32 балів.

Тест проводиться на платформі дистанційного навчання Moodle і питання можуть бути різної форми, які можна реалізувати в Moodle.

4) Таблиця відповідності рейтингових балів оцінкам за університетською шкалою

Кількість балів	Оцінка
95...100	Відмінно
85...94	Дуже добре
75...84	Добре
65...74	Задовільно
60...64	Достатньо
Менше 60	Незадовільно

10. Додаткова інформація з дисципліни (освітнього компонента)

Приклади тестових питань для модульної контрольної роботи

1. Стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації називається …

a) конфіденційність інформації;
b) розмежування доступу;
c) захищена комп'ютерна система;
d) безпека інформації;
e) жодної правильної відповіді.

2. Сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС називається …

a) комплексна система захисту інформації;
b) комплекс засобів захисту;
c) захист інформації в АС;
d) політика безпеки інформації;
e) жодної правильної відповіді.

3. Частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів називається…

a) керування доступом;
b) санкціонований доступ до інформації;
c) повноваження;
d) правила розмежування доступу;
e) жодної правильної відповіді.

4. Властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом називається …

a) конфіденційність інформації;
b) доступність інформації;
c) можливість спостереження інформації;
d) цілісність інформації;
e) жодної правильної відповіді.

5. Функція ймовірності реалізації певної загрози, виду і величини завданих збитків називається …

a) ризик;
b) вразливість системи;
c) критерій оцінки захищеності;
d) функціональний профіль;
e) жодної правильної відповіді.

6. Процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту називається …

a) авторизація;
b) ідентифікація;

c) автентифікація;
d) тестування на проникнення;
e) жодної правильної відповіді.

7. Вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до іншого і/або відбувається зміна стану системи називається …

a) тип доступу ;
b) розмежування доступу;
c) доступ до інформації;
d) доступність;
e) жодної правильної відповіді.

8. Яку назву з наведеного нижче списку функціональних можливостей деякого універсального комплексу мережевого екранування принципово йому не притаманна …

a) кешування результатів запитів на доступ до об'єктів інформаційних сервісів (ресурсів) у зовнішній чи внутрішній мережі;
b) фільтрація пакетів;
c) трансляція адрес, портів;
d) протоколювання параметрів мережевого трафіку, який підлягає маршрутизації між зовнішньою та внутрішньою мережею;
e) жодної правильної відповіді.

9. Наука про методи захисту інформації шляхом перетворення форми її представлення – …

a) криптографія;
b) криптологія;
c) криптоаналіз;
d) криптосистема;
e) криптоперетворення.

10. До негативних рис практичного використання симетричних криптосистем слід відносити …

a) непридатність для функціонування у складі сучасних криптопротоколів;
b) низьку, у порівняння з асиметричними, продуктивність шифрування значних масивів даних, потоків даних значної інтенсивності;
c) проблемність розподілу секретного ключа між абонентами;
d) і a), і c);
e) жодної правильної відповіді.

11. Який з наведеного нижче списку алгоритмів використовується у складі криптопротоколу SSH2 для вироблення на етапі автентифікації ssh-клієнта та вироблення спільного секретного ключа сеансу?

a) Поліга-Хелмана;
b) Гиллоу-Куіскуотера;
c) Ель-Гамаля;
d) Діффі-Хелмана;
e) жодної правильної відповіді.

12. В якому з наведеного нижче списку крипто алгоритмів конструктивно застосовується найменша довжина ключа?

a) SHA;
b) RSA;
c) IDEA;
d) EGSA;
e) DES.

13. Яку назву з наведеного нижче списку слід віднести до множини понять криптопротоколів канального рівня?

a) Secure Sockets Layer;

b) Secure MIME;
c) IP Security;
d) Simple Key management for the Internet Protocol;
e) жодної правильної відповіді.

14. Тунельний режим функціонування крипто протоколів транспортного рівня передбачає інкапсуляцію IP-пакета, при транспортуванні через іншу логічну мережу,…

a) в іншій IP-пакет без шифрування;
b) у зашифрованій формі в іншій IP-пакет;
c) в іншій IP-пакет з шифруванням заголовку цього пакету перед передачею;
d) здійснюючи шифрування тільки його вмісту (корисних даних), але не заголовку;
e) жодної правильної відповіді.

15. Яке з наведеного нижче списку понять не слід відносити до складу деякого, узагальненого ідентифікаційного сертифікату абстрагуючись від вимог конкретного стандарту …

a) адреса електронної пошти власника ідентифікаційного сертифікату;
b) термін дії ідентифікаційного сертифікату;
c) ідентифікатор повноважень власника ідентифікаційного сертифікату;
d) відкритий ключ власника ідентифікаційного сертифікату;
e) жодної правильної відповіді.

16. Яку назву з наведеного нижче списку не слід відносити до переліку стандартних процедур поводження з ідентифікаційними сертифікатами, що розглядаються у контексті функціонування тієї чи іншої інфраструктури відкритих ключів?

a) верифікація;
b) видання;
c) публікація;
d) відкликання;
e) відновлення.

17. Поняття "самопідписаний ідентифікаційний сертифікат" притаманне …

a) ISO ITU-T X.509 v.1;
b) ISO ITU-T X.509 v.2;
c) ISO ITU-T X.509 v.3;
d) PGP;
e) жодної правильної відповіді.

18. Абревіатура IPS є скороченням від …

a) Improving Prevention Subsystem;
b) Instruction Prevention System;
c) Insider Prevention Subsystem;
d) Intrusion Penetration System;
e) жодної правильної відповіді.

19. Позитивними рисами програмно-технічних засобів (систем) виявлення спроб реалізації загроз безпеці інформації кібернетичної природи в ТКС, функціонування яких засновано на методі аналізу сигнатур вважаються …

a) більша продуктивність виявлення за їх відомими описами (правилами, сигнатурами) у порівняні з методом аналізу аномалій;
b) здатність виявляти нові (невідомі раніше) сценарії спроб реалізації загроз безпеці інформації кібернетичної природи в ТКС;
c) низька ймовірність хибної ідентифікації спроб реалізації загроз за їх відомими описами (правилами, сигнатурами);
d) і a), і c);
e) жодної правильної відповіді.

20. Процес обробки реєстраційних даних про однотипні події результатом якого є показник їх інтенсивності прийнято називати …

a) нормалізація;
b) фільтрація;
c) агрегація;
d) кореляція;
e) візуалізація.

Робочу програму навчальної дисципліни (силабус):

Складено:
к.т.н., доц. Могильний Сергій Борисович.
Ухвалено:
Засіданням кафедри інформаційно-комунікаційних технологій та систем (протокол № 9 від 19 травня 2022 року)

Погоджено:
Методичною комісією навчально-наукового інституту телекомунікаційних систем
(протокол № 4 від 02 червня 2022 року)