Робоча програма дисципліни «Захист інформації в інформаційно-комунікаційних системах»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

3

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Захист інформації в інформаційно-комунікаційних системах

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 90 годин / 3 кредити ЄКТС

Модулів: 3 змістовних блоки

Призначення дисципліни

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» формує у студентів системне розуміння принципів, методів та засобів захисту інформації в сучасних ІКС. Курс охоплює теоретичні основи інформаційної безпеки, нормативно-правову базу, технічні та криптографічні механізми захисту, а також практичні аспекти побудови комплексних систем захисту інформації.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» за освітньою програмою «Організація захисту інформації в інформаційно-комунікаційних системах» та забезпечує формування фахових компетентностей у галузі кібербезпеки.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації про загрози та вразливості ІКС: виявлення ризиків, порівняння альтернативних методів захисту, формування обґрунтованих висновків щодо вибору засобів безпеки.

Комунікація

Здатність до усної та письмової комунікації: чітко описувати загрози та механізми захисту, аргументовано обґрунтовувати проектні рішення, оформлювати звіти, технічні завдання та аналітичні записки з питань захисту інформації.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки звітів, лабораторних робіт і дослідницьких проектів у сфері захисту інформації.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групового аналізу сценаріїв кіберзагроз, проектування систем захисту та вироблення спільних рекомендацій щодо забезпечення безпеки ІКС.

Студент повинен вміти: аналізувати інформацію про загрози та засоби захисту; виділяти головне та узагальнювати результати; планувати власну діяльність і дотримуватися дедлайнів; коректно спілкуватися з викладачами та одногрупниками; брати участь у командній роботі та розподіляти обов'язки.

Фахові компетентності

Основи захисту інформації

Розуміння сутності та закономірностей забезпечення захисту інформації в ІКС, класифікації загроз, вразливостей та атак. Знання принципів побудови систем захисту, вміння аналізувати ризики та оцінювати рівень захищеності інформаційних систем.

Криптографічний захист

Здатність застосовувати криптографічні методи та алгоритми для забезпечення конфіденційності, цілісності та автентичності інформації; використовувати засоби криптографічного захисту та електронного підпису відповідно до чинних стандартів.

Технічні засоби захисту

Знання та вміння застосовувати технічні засоби захисту інформації: міжмережеві екрани, системи виявлення вторгнень, засоби аутентифікації та контролю доступу, антивірусний захист та засоби моніторингу ІКС.

Нормативно-правова база

Орієнтування в нормативно-правовій базі України у сфері захисту інформації та кібербезпеки; використання вітчизняних і міжнародних стандартів (ДСТУ, ISO/IEC) для побудови комплексних систем захисту інформації в ІКС.

Результати навчання

01

Пояснення базових понять

Пояснювати сутність ключових понять та явищ: інформаційна безпека, конфіденційність, цілісність, доступність, загроза, вразливість, атака, криптографічний захист, автентифікація, авторизація, комплексна система захисту інформації.

02

Аналіз загроз та вразливостей

Характеризувати основні класи загроз та вразливостей ІКС, застосовувати методи оцінювання ризиків інформаційної безпеки, визначати актуальні загрози для конкретної інформаційної системи та обирати адекватні засоби захисту.

03

Проектування засобів захисту

Проектувати та впроваджувати технічні та організаційні заходи захисту інформації в ІКС; застосовувати криптографічні алгоритми, налаштовувати засоби мережевого захисту та системи контролю доступу.

04

Робота з нормативними документами

Орієнтуватися у нормативно-правовій базі України та міжнародних стандартах у сфері захисту інформації; використовувати нормативні документи для обґрунтування та розробки комплексних систем захисту інформації.

МОДУЛЬ 1

Теоретичні основи захисту інформації в ІКС

1 — Тема 1.1

Основні поняття інформаційної безпеки. Класифікація загроз та вразливостей ІКС. Модель порушника.

2 — Тема 1.2

Нормативно-правова база захисту інформації в Україні. Вітчизняні та міжнародні стандарти (ДСТУ, ISO/IEC 27001).

3 — Тема 1.3

Криптографічні методи захисту інформації: симетричні та асиметричні алгоритми, хешування, електронний підпис.

4 — Тема 1.4

Протоколи захисту інформації у мережах. PKI. Захист каналів передачі даних (SSL/TLS, VPN, IPSec).

МОДУЛЬ 1 · ТЕМА 1.1

Основні поняття інформаційної безпеки. Класифікація загроз

Лекційний матеріал (4 год.)

Лекція 1: Поняття інформаційної безпеки, її складові: конфіденційність, цілісність, доступність (тріада CIA). Базові терміни та визначення. Поняття активів, загроз, вразливостей та ризиків. Класифікація загроз безпеці інформації в ІКС.

Лекція 2: Модель порушника: типи зловмисників, мотивація, класифікація. Методи та засоби реалізації атак. Огляд актуальних кіберзагроз (APT, ransomware, фішинг, DDoS). Поняття кіберінциденту та управління інцидентами.

Ключові питання лекцій

- Тріада CIA та розширені моделі інформаційної безпеки
- Класифікація загроз за джерелом, характером та наслідками
- Типи вразливостей ІКС: технічні, організаційні, людський чинник
- Модель порушника та методи реалізації атак
- Актуальний ландшафт кіберзагроз для українських ІКС

Практичне заняття (1 год.)

Завдання 1. Аналіз реальних кіберінцидентів в українських ІКС: ідентифікація типу загрози, вразливості та наслідків. Класифікація за стандартизованими таксономіями.

Завдання 2. Побудова моделі загроз для навчальної інформаційної системи: визначення активів, загроз, вразливостей та оцінка ризиків.

Самостійна робота (10 год.)

- Опрацювання: Корченко О. Г. та ін. «Захист інформації в інформаційно-телекомунікаційних системах» — розділ «Основи безпеки»
- Підготовка реферату: «Актуальні кіберзагрози для критичної інфраструктури України»
- Складання глосарію термінів з інформаційної безпеки за ДСТУ

Очікуваний результат: студент вміє характеризувати основні поняття інформаційної безпеки, класифікувати загрози та будувати базову модель загроз для ІКС.

МОДУЛЬ 1 · ТЕМА 1.2

Нормативно-правова база захисту інформації в Україні

1

Законодавство

Закони України про інформацію, захист інформації в ІКС, кібербезпеку.

2

НД ТЗІ

Нормативні документи системи технічного захисту інформації ДССЗЗІ України.

3

ДСТУ / ISO

Вітчизняні стандарти ДСТУ та міжнародні ISO/IEC 27001, 27002, 27005.

4

КСЗІ

Атестація та введення в дію комплексної системи захисту інформації.

Лекційний матеріал (4 год.)

Правові основи захисту інформації: Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон «Про кібербезпеку», «Про основні засади забезпечення кібербезпеки України». Нормативні документи ДССЗЗІ. Стандарти ДСТУ ISO/IEC 27001, 27002, 27005. Вимоги до КСЗІ: порядок створення, атестації та введення в дію. Ролі та відповідальність суб'єктів захисту інформації.

Практика (1 год.) та СРС (10 год.)

Практика: Аналіз вимог НД ТЗІ до класу захищеності ІКС; визначення переліку необхідних організаційних і технічних заходів для конкретної ІКС відповідно до нормативних вимог.

СРС: Опрацювання: Замула О. А., Горбенко Ю. І. «Комплексні системи захисту інформації» (2023); підготовка порівняльного аналізу вимог ДСТУ ISO/IEC 27001 та НД ТЗІ України до систем захисту інформації.

МОДУЛЬ 1 · ТЕМИ 1.3–1.4

Криптографічний захист та захищені протоколи

Тема 1.3 — Криптографічний захист (Лекції 5–6, 4 год.)

Симетричні алгоритми шифрування: DES, 3DES, AES, ДСТУ 7624 (Калина). Асиметричні алгоритми: RSA, ECC, ДСТУ 4145 (криптосистема на основі еліптичних кривих). Хеш-функції: MD5, SHA-2/3, ДСТУ 7564 (Купина). Алгоритм електронного цифрового підпису. Управління ключами: генерація, розподіл, зберігання, знищення.

Практика (1 год.): Реалізація симетричного та асиметричного шифрування за допомогою програмних засобів; генерація ключових пар та перевірка електронного підпису.

СРС (10 год.): Опрацювання: Горбенко І. Д., Горбенко Ю. І. «Прикладна криптологія» (2022); підготовка реферату «Порівняльний аналіз вітчизняних та міжнародних криптографічних стандартів».

Тема 1.4 — Захищені протоколи (Лекції 7–8, 4 год.)

Інфраструктура відкритих ключів (PKI): центри сертифікації, цифрові сертифікати X.509, списки відкликаних сертифікатів. Протокол SSL/TLS: принципи роботи, версії, налаштування. Протоколи VPN (IPSec, OpenVPN). Захист бездротових мереж: WPA2/WPA3. Протоколи автентифікації: Kerberos, RADIUS, OAuth 2.0, OpenID Connect.

Практика (1 год.): Налаштування захищеного з'єднання TLS; аналіз сертифікатів та ланцюжків довіри; конфігурація VPN-тунелю в лабораторному середовищі.

СРС (10 год.): Опрацювання: Нестеренко Г. «Інформаційна безпека: курс лекцій» (Київ: НАУ, 2022) — розділи про протоколи захисту; підготовка порівняльної таблиці протоколів захищеної передачі даних.

МОДУЛЬ 2

Технічні засоби та методи захисту інформації в ІКС

Тема 2.1

Мережевий захист: міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), DMZ.

Тема 2.2

Управління доступом: ідентифікація, автентифікація, авторизація. Моделі розмежування доступу. MFA.

Тема 2.3

Захист від шкідливого програмного забезпечення. Антивірусні засоби. Пісочниці. EDR/XDR рішення.

Тема 2.4

Моніторинг та аудит безпеки ІКС. SIEM-системи. Управління вразливостями. Тестування на проникнення.

МОДУЛЬ 2 · ТЕМА 2.1

Мережевий захист: ME, IDS/IPS, архітектура безпечних мереж

Лекційний матеріал (4 год.)

Мережева безпека: загрози на мережевому рівні, сегментація мережі, DMZ. Міжмережеві екрани (Firewall): типи (пакетний фільтр, stateful inspection, NGFW), принципи налаштування, правила фільтрації. Системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS): мережеві та хостові, сигнатурний та аномальний аналіз. WAF — міжмережевий екран для веб-застосунків. Захист від DDoS-атак. Мережева архітектура з урахуванням вимог безпеки: Zero Trust.

Ключові питання

- Принципи мережевої сегментації та DMZ
- Класифікація та налаштування міжмережевих екранів
- IDS/IPS: методи виявлення та реагування на вторгнення
- Концепція Zero Trust та її реалізація в ІКС
- Захист від DDoS-атак: методи та засоби

Практичне заняття (1 год.)

Завдання 1. Налаштування правил міжмережевого екрану для захисту навчальної мережі: розробка та перевірка ACL, тестування фільтрації трафіку.

Завдання 2. Аналіз сигнатур та алертів IDS/IPS у навчальному середовищі Snort/Suricata; виявлення аномального трафіку та класифікація інцидентів.

Самостійна робота (10 год.)

- Опрацювання: Корченко О. Г., Архипов О. Є. «Системи виявлення вторгнень» (2023, КПІ) — розділ «Методи виявлення аномалій»
- Підготовка реферату: «Zero Trust Architecture: принципи та практика впровадження»
- Складання схеми безпечної мережевої архітектури для підприємства

Очікуваний результат: студент вміє проектувати мережеву архітектуру з урахуванням вимог безпеки, налаштовувати засоби мережевого захисту та аналізувати мережевий трафік.

МОДУЛЬ 2 · ТЕМА 2.2

Управління доступом та автентифікація

Ідентифікація

Визначення суб'єкта: логін, UUID, біометричні дані. Унікальність ідентифікатора.

Авторизація

Надання прав доступу: моделі DAC, MAC, RBAC, ABAC. Принцип найменших привілеїв.

IAM-система

Identity and Access Management: централізоване управління обліковими записами та правами.

Автентифікація

Підтвердження особи: пароль, токен, біометрія. MFA — багатофакторна автентифікація.

Аудит

Журналювання дій: хто, що, коли. Незаперечність та цілісність журналів.

Лекційний матеріал (4 год.)

Ідентифікація, автентифікація та авторизація як ключові елементи управління доступом. Фактори автентифікації: знання, володіння, біометрія. Багатофакторна автентифікація (MFA). Моделі розмежування доступу: дискреційна (DAC), мандатна (MAC), рольова (RBAC), атрибутна (ABAC). Принцип найменших привілеїв. IAM-системи: Active Directory, LDAP. Привілейований доступ (PAM). Single Sign-On (SSO).

Практика (1 год.) та СРС (10 год.)

Практика: Налаштування рольової моделі доступу в навчальному середовищі; реалізація MFA; аналіз журналів аудиту та виявлення підозрілих подій доступу.

СРС: Опрацювання: Замула О. А., Горбенко Ю. І. «Комплексні системи захисту інформації» (2023) — розділ «Управління доступом»; підготовка аналітичної записки «Порівняльний аналіз моделей розмежування доступу для корпоративних ІКС».

МОДУЛЬ 2 · ТЕМИ 2.3–2.4

Захист від шкідливого ПЗ та моніторинг безпеки

Тема 2.3 — Захист від шкідливого ПЗ (Лекції 13–14, 4 год.)

Класифікація шкідливого програмного забезпечення: віруси, трояни, хробаки, ransomware, spyware, rootkit, APT. Методи виявлення: сигнатурний аналіз, евристичний аналіз, поведінковий аналіз. Антивірусні рішення та EDR/XDR-платформи. Пісочниці (Sandbox) для безпечного аналізу підозрілих файлів. Захист електронної пошти та веб-трафіку. Управління оновленнями та патчами. Принципи безпечної розробки ПЗ (SSDLC).

Практика (1 год.): Аналіз зразків шкідливого ПЗ у безпечному середовищі (статичний та динамічний аналіз); налаштування антивірусного захисту та перевірка ефективності виявлення.

СРС (5 год.): Опрацювання: Коваленко О. М. «Аналіз шкідливого програмного забезпечення: методи та інструменти» (2023); підготовка звіту про результати аналізу зразка шкідливого ПЗ.

Тема 2.4 — Моніторинг та аудит безпеки (Лекції 15–16, 4 год.)

Моніторинг безпеки ІКС: цілі, завдання, методи. SIEM-системи (Security Information and Event Management): архітектура, принципи роботи, кореляція подій. SOC (Security Operations Center): структура, процеси, метрики. Управління вразливостями: сканування, оцінка, пріоритизація, усунення. Тестування на проникнення (Penetration Testing): методологія, інструменти, звітність. Аудит безпеки та оцінювання відповідності. Bug Bounty програми.

Практика (1 год.): Робота з SIEM-системою: налаштування правил кореляції, аналіз подій безпеки та виявлення інцидентів; сканування вразливостей у навчальній мережі.

СРС (5 год.): Підготовка аналітичної записки «SIEM-системи в Ukrainian SOC: практика впровадження та ефективність».

МОДУЛЬ 3

Організація захисту інформації: комплексні системи та управління

Тема 3.1

Побудова комплексної системи захисту інформації (КСЗІ). Концепція і технічне завдання на КСЗІ. Атестація.

Тема 3.2

Управління інформаційною безпекою: СУІБ (ISO/IEC 27001). Оцінювання та управління ризиками. ISMS.

Тема 3.3

Захист хмарних середовищ та сучасних ІКС. Cloud Security, IoT Security, безпека мікросервісів та DevSecOps.

Тема 3.4

Реагування на кіберінциденти та відновлення. BCP/DR. Форензика. Управління кіберризиками організації.

МОДУЛЬ 3 · ТЕМА 3.1

Побудова комплексної системи захисту інформації (КСЗІ)

Лекційний матеріал (4 год.)

Поняття КСЗІ та її складові: організаційні, технічні, криптографічні та програмні засоби. Порядок створення КСЗІ відповідно до НД ТЗІ: концепція безпеки, технічне завдання, проектування, впровадження, атестація. Класи захищеності автоматизованих систем. Документальне забезпечення КСЗІ. Роль служби захисту інформації (СЗІ). Контроль стану безпеки. Ліцензування у сфері технічного захисту інформації. Порядок атестації КСЗІ та отримання атестата відповідності.

Ключові питання

- Структура та складові КСЗІ
- Порядок проектування та впровадження КСЗІ
- Класифікація автоматизованих систем за класами захищеності
- Документальне забезпечення та атестація КСЗІ
- Роль та функції служби захисту інформації

Практичне заняття (2 год.)

Завдання 1. Розробка концепції безпеки та технічного завдання на КСЗІ для модельної організації: визначення класу захищеності, переліку загроз та вимог до засобів захисту.

Завдання 2. Складання переліку організаційних та технічних заходів захисту відповідно до вимог НД ТЗІ для визначеного класу ІКС.

Самостійна робота (10 год.)

- Опрацювання: Замула О. А., Горбенко Ю. І. «Комплексні системи захисту інформації: навч. посіб.» (2023) — розділи «Проектування КСЗІ», «Атестація»
- Підготовка реферату: «Порядок атестації КСЗІ в Україні: нормативні вимоги та практика»
- Аналіз вимог НД ТЗІ 2.5-004 до класів захищеності автоматизованих систем

Очікуваний результат: студент вміє проектувати КСЗІ, розробляти концепцію безпеки та технічне завдання, орієнтуватися у вимогах нормативних документів ТЗІ.

МОДУЛЬ 3 · ТЕМА 3.2

Управління інформаційною безпекою (СУІБ / ISO 27001)

Plan (Планування)

Визначення контексту, оцінка ризиків, постановка цілей безпеки, розробка плану обробки ризиків.

Do (Впровадження)

Реалізація заходів безпеки, навчання персоналу, впровадження контролів відповідно до Додатку A ISO 27001.

Check (Перевірка)

Внутрішній аудит, аналіз показників ефективності, моніторинг контролів безпеки, оцінка відповідності.

Act (Вдосконалення)

Коригувальні та запобіжні дії, перегляд СУІБ, безперервне вдосконалення системи управління.

Лекційний матеріал (4 год.)

Система управління інформаційною безпекою (СУІБ): цикл PDCA. ISO/IEC 27001:2022 — вимоги до СУІБ. ISO/IEC 27002:2022 — практика управління заходами безпеки. ISO/IEC 27005 — управління ризиками ІБ. Оцінювання ризиків: методики (кількісна, якісна), матриця ризиків. Обробка ризиків: прийняття, уникнення, передача, зменшення. Сертифікація за ISO 27001. Метрики ефективності СУІБ.

Практика (2 год.) та СРС (10 год.)

Практика: Проведення оцінювання ризиків інформаційної безпеки для модельної організації за методикою ISO/IEC 27005: ідентифікація активів, загроз, вразливостей, оцінка ймовірності та наслідків, формування реєстру ризиків.

СРС: Опрацювання: Горбенко І. Д., Горбенко Ю. І. «Стандарти інформаційної безпеки: ISO/IEC 27000-серія» (2022); підготовка аналітичної записки «Впровадження СУІБ в українських організаціях: виклики та кращі практики».

МОДУЛЬ 3 · ТЕМИ 3.3–3.4

Захист хмарних середовищ та реагування на інциденти

Тема 3.3 — Захист хмарних та сучасних ІКС (Лекції 21–22, 4 год.)

Моделі хмарних обчислень (IaaS, PaaS, SaaS) та питання безпеки. Модель спільної відповідальності (Shared Responsibility Model). Cloud Security Alliance (CSA) та стандарти хмарної безпеки. Захист контейнеризованих середовищ (Docker, Kubernetes). DevSecOps: інтеграція безпеки в процес розробки. Безпека IoT та промислових ІКС (ICS/SCADA). Захист мобільних пристроїв (MDM). Безпека мікросервісної архітектури. API Security.

Практика (2 год.): Аудит безпеки хмарного середовища (AWS/Azure/GCP); налаштування Security Groups, IAM-ролей; аналіз Cloud Security Posture Management (CSPM) рекомендацій.

СРС (5 год.): Опрацювання: Коваленко О. М. «Хмарна безпека: архітектура та практики захисту» (2023); підготовка реферату «Безпека IoT-пристроїв в промислових ІКС України».

Тема 3.4 — Реагування на інциденти та форензика (Лекції 23–24, 4 год.)

Управління кіберінцидентами: цикл NIST SP 800-61 (підготовка, виявлення, стримування, усунення, відновлення, пост-інцидентний аналіз). Computer Forensics: принципи збору та дослідження цифрових доказів, ланцюг зберігання доказів (Chain of Custody). Планування безперервності бізнесу (BCP) та відновлення після катастроф (DRP). RTO та RPO. Playbook та Runbook для реагування на типові інциденти. CERT-UA та співпраця з державними структурами.

Практика (2 год.): Розробка Playbook для реагування на ransomware-атаку; аналіз дампу пам'яті та образу диску у навчальному форензика-завданні (Volatility, Autopsy).

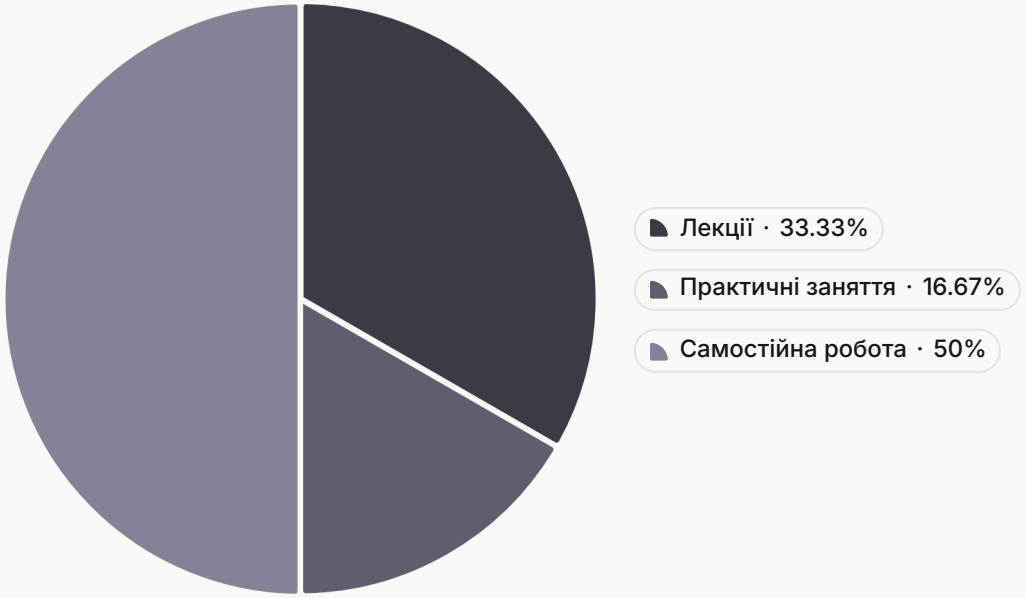
СРС (5 год.): Підготовка аналітичної записки «Реагування на кіберінциденти: досвід CERT-UA та уроки для організацій».

Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Основи ІБ та загрози	4	1	10
	Тема 1.2 — Нормативно-правова база	4	1	10
	Тема 1.3 — Криптографічний захист	4	1	5
	Тема 1.4 — Захищені протоколи та PKI	4	1	5
Модуль 2	Тема 2.1 — Мережевий захист	4	2	5
	Тема 2.2 — Управління доступом	4	2	5
	Тема 2.3 — Захист від шкідливого ПЗ	4	2	5
	Тема 2.4 — Моніторинг та аудит безпеки	4	2	5
Модуль 3	Тема 3.1 — КСЗІ: проектування та атестація	4	1	5
	Тема 3.2 — СУІБ / ISO 27001	4	1	5
	Тема 3.3 — Хмарна безпека та DevSecOps	4	1	5
	Тема 3.4 — Реагування на інциденти. Форензика	4	1	5
Разом	**12 тем**	**48**	**16**	**—**

Загальний обсяг: 90 годин = 3 кредити ЄКТС. Лекції — 30 год., практичні — 15 год., самостійна робота — 45 год. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **90 годин (3 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

Лекції — 30 год. (33%)

Системне подання теоретичного матеріалу з використанням наочних схем, діаграм і прикладів з практики забезпечення інформаційної безпеки вітчизняних організацій.

Практичні — 15 год. (17%)

Відпрацювання практичних навичок: налаштування засобів захисту, аналіз вразливостей, розробка КСЗІ, оцінювання ризиків та реагування на інциденти.

Самостійна робота — 45 год. (50%)

Поглиблене вивчення, підготовка завдань, робота з нормативними документами та науковою літературою. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками з захисту інформації (Горбенко, Замула, Корченко, Коваленко та ін.), нормативними документами ТЗІ та НД ДССЗЗІ, науковими статтями у фахових виданнях. Студент конспектує ключові положення та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (оцінювання ризиків, аналіз вразливостей, порівняння засобів захисту); творчих завдань — есе, аналітичні записки, звіти з аналізу реальних кіберінцидентів та розробки рекомендацій щодо захисту ІКС.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: ДССЗЗІ України (**cip.gov.ua**), CERT-UA (**cert.gov.ua**), Верховної Ради (**zakon.rada.gov.ua**), Національної бібліотеки (**nbuv.gov.ua**). Аналіз звітів про кіберінциденти та кіберзагрози.

Підготовка до занять

Підготовка до практичних занять (опрацювання нормативних документів, технічної документації на засоби захисту); підготовка до тестувань (ключові терміни, стандарти, алгоритми); підготовка до контрольних робіт за кожним модулем.

Форми контролю знань

1	2	3
Поточний контроль	**Проміжний контроль**	**Підсумковий контроль**
Завдання: тестові та аналітичні вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість звітів з практичних занять та рівень засвоєння матеріалу. Проводиться після кожної теми у формі тестування (10–15 питань) або усного опитування з демонстрацією практичних навичок.	Самостійна робота — комплексне завдання або реферат, які охоплюють теми змістовного модуля (теоретичні питання, аналіз нормативних документів, розробка заходів захисту для модельної ІКС). Оцінюються повнота відповіді, аргументованість та практична цінність висновків. Проводиться після завершення кожного модуля.	Залік/іспит відповідно до навчального плану. Форма — тестування та письмові відповіді на питання, або захист комплексного практичного завдання. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Захист інформації в ІКС» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок, необхідних для майбутньої професійної діяльності у сфері комп'ютерної інженерії та організації захисту інформації.

Лекції

Системне подання теоретичного матеріалу з використанням схем, діаграм атак, топологій мереж та прикладів реальних кіберінцидентів; студенти ведуть конспекти та задають запитання.

Практичні заняття

Відпрацювання практичних навичок у навчальних лабораторіях та віртуальних середовищах: налаштування засобів захисту, аналіз трафіку, форензика, оцінювання ризиків.

Кейс-стаді

Аналіз реальних кіберінцидентів (зокрема атак на українські ІКС); студенти виявляють вектори атак, оцінюють наслідки та пропонують заходи захисту.

Дискусії

Обговорення дискусійних питань кібербезпеки; розвиток критичного мислення, аргументації та вміння обґрунтовувати технічні та організаційні рішення із захисту інформації.

Самостійне дослідження

Підготовка аналітичних записок, рефератів і звітів з питань захисту інформації; розвиток навичок самостійного пошуку та систематизації технічної та нормативної інформації.

CTF та змагання

Участь у навчальних Capture The Flag змаганнях та кіберполігонах для розвитку практичних навичок тестування безпеки в контрольованому середовищі.

Усі методи спрямовані на формування компетентностей, передбачених освітньо-професійною програмою «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література — Підручники та посібники (2022–2024 рр.)

1. Горбенко І. Д., Горбенко Ю. І.

Прикладна криптологія: теорія, практика, застосування: підручник. — 2-ге вид., перероб. та доп. — Харків : Форт, 2022. — 880 с. ISBN 978-617-629-236-8

2. Замула О. А., Горбенко Ю. І.

Комплексні системи захисту інформації: проектування, впровадження, атестація: навч. посіб. — Харків : ХНУРЕ, 2023. — 312 с.

3. Нестеренко Г. О.

Інформаційна безпека: курс лекцій для студентів ЗВО. — Київ : НАУ, 2022. — 268 с.

4. Коваленко О. М.

Аналіз шкідливого програмного забезпечення: методи та інструменти: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2023. — 248 с.

5. Корченко О. Г., Архипов О. Є.

Системи виявлення вторгнень: моделі, методи, технології: монографія. — Київ : НАУ, 2023. — 296 с.

6. Коваленко О. М.

Хмарна безпека: архітектура та практики захисту: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2023. — 224 с.

7. Горбенко І. Д., Горбенко Ю. І.

Стандарти інформаційної безпеки: ISO/IEC 27000-серія: навч. посіб. — Харків : ХНУРЕ, 2022. — 196 с.

8. Корченко О. Г. та ін.

Захист інформації в інформаційно-телекомунікаційних системах: підручник для ЗВО. — 3-тє вид., перероб. — Київ : НАУ, 2022. — 420 с.

Додаткова література та наукові статті

9. Петров В. В., Стасюк О. І.

Методи та засоби забезпечення кібербезпеки критичної інфраструктури. — Київ : ІПРІ НАН України, 2023. — 198 с. *Рекомендується для тем 2.1, 3.3–3.4.*

10. Лукацький А. В., Борисенко Н. В.

Управління інцидентами інформаційної безпеки: практичний посібник. — Київ : Університет «Україна», 2023. — 184 с. *Рекомендується для теми 3.4.*

11. Рибальченко Л. В., Гребенюк А. М.

Основи управління інформаційною безпекою: навч. посіб. — 2-ге вид., доп. — Дніпро : ДДУВС, 2022. — 216 с. *Рекомендується для тем 1.2, 3.1–3.2.*

12. Журнал «Захист інформації» (НАУ)

Фахове видання у сфері технічного та криптографічного захисту інформації. Статті за 2022–2024 рр. — **jrnl.nau.edu.ua**. *Рекомендується для всіх модулів.*

Нормативно-правова база

- Закон України «Про захист інформації в інформаційно-комунікаційних системах»

  № 80/94-ВР від 05.07.1994 (в редакції від 2022). Основоположний закон у сфері ТЗІ. **zakon.rada.gov.ua**

- Закон України «Про основні засади забезпечення кібербезпеки України»

  № 2163-VIII від 05.10.2017. Визначає засади державної політики у сфері кібербезпеки. **zakon.rada.gov.ua**

- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах»

  Нормативний документ ДССЗЗІ України щодо класів захищеності автоматизованих систем. **cip.gov.ua**

- ДСТУ ISO/IEC 27001:2015 «Системи управління інформаційною безпекою»

  Вітчизняний стандарт управління ІБ на основі міжнародного ISO/IEC 27001. **zakon.rada.gov.ua**

- Стратегія кібербезпеки України, затверджена Указом Президента України № 447/2021

  Стратегічний документ у сфері кібербезпеки держави на 2021–2025 роки. **zakon.rada.gov.ua**

Офіційні ресурси та фахові видання

ДССЗЗІ України

cip.gov.ua — Державна служба спеціального зв'язку та захисту інформації: нормативні документи, НД ТЗІ, ліцензування.

CERT-UA

cert.gov.ua — Урядова команда реагування на комп'ютерні надзвичайні події: звіти про кіберінциденти, бюлетені безпеки, рекомендації.

Верховна Рада України

zakon.rada.gov.ua — нормативно-правова база у сфері захисту інформації, кібербезпеки та ІКС.

Національна бібліотека ім. В. І. Вернадського

nbuv.gov.ua — електронні ресурси, наукові статті та монографії з інформаційної безпеки та захисту ІКС.

Журнал «Захист інформації»

jrnl.nau.edu.ua — провідне фахове видання НАУ з питань технічного та криптографічного захисту інформації.

«Безпека інформації» (ДУТ)

Фахове видання Державного університету телекомунікацій з питань захисту інформації в телекомунікаційних системах та мережах.

Міністерство освіти і науки України

mon.gov.ua — освітні стандарти, навчальні програми та методичні матеріали для спеціальності 123 «Комп'ютерна інженерія».

Інститут кібербезпеки та захисту інформації КПІ

ibb.kpi.ua — наукові публікації, навчальні матеріали, результати досліджень у сфері кібербезпеки та захисту ІКС.

Зв'язок дисципліни зі спеціальністю 123 «Комп'ютерна інженерія»

Чому «Захист інформації в ІКС» для інженерів?

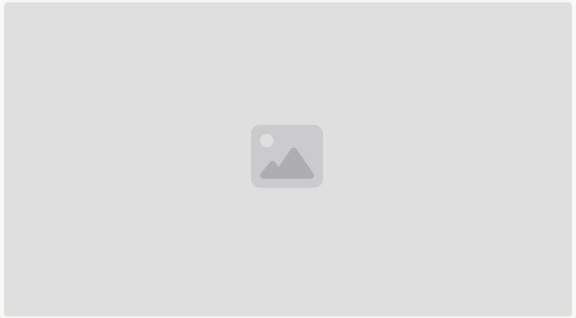
Дисципліна є невід'ємною складовою підготовки бакалаврів зі спеціальності 123 «Комп'ютерна інженерія». Сучасний інженер створює системи, які зберігають, обробляють та передають чутливі дані — тому знання принципів захисту інформації є обов'язковою компетентністю, а не додатковою.

В умовах активної кібервійни проти України та зростання кількості кіберзагроз для вітчизняних організацій, кожен фахівець у сфері комп'ютерної інженерії повинен вміти проектувати захищені системи та реагувати на загрози безпеці.

Практичне значення для майбутньої кар'єри

- Проектування захищених ІКС з урахуванням вимог НД ТЗІ та ДСТУ ISO/IEC 27001
- Розробка безпечного програмного забезпечення (Secure SDLC, DevSecOps)
- Участь у створенні та атестації КСЗІ в державних та комерційних організаціях
- Аналіз вразливостей та тестування на проникнення (Pentesting)
- Реагування на кіберінциденти та відновлення роботи ІКС після атак
- Кар'єра в SOC, CERT, службах ТЗІ та підрозділах кібербезпеки

Ключові компетентності курсу — Підсумок



Курс охоплює всі ключові аспекти захисту інформації в ІКС — від теоретичних основ і правової бази до технічних засобів захисту та організації комплексних систем безпеки — і формує у студентів цілісне розуміння сучасної практики забезпечення кібербезпеки.

Бажаємо успіхів у вивченні захисту інформації!

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

12

Тем

У 3 змістовних модулях

8

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Безпека — це не продукт, який можна купити, а процес, якому треба постійно слідувати.» — Брюс Шнайєр

Спеціальність 123 · Комп'ютерна інженерія · Бакалавр · 3 кредити ЄКТС · ОП: Організація захисту інформації в ІКС