Робоча програма дисципліни «Захист конфіденційних даних»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

4

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Захист конфіденційних даних

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки

Призначення дисципліни

Дисципліна «Захист конфіденційних даних» формує у студентів системне розуміння принципів, методів та інструментів захисту конфіденційної інформації в інформаційно-комунікаційних системах. Курс охоплює правові засади, технічні механізми та організаційні заходи забезпечення конфіденційності даних відповідно до вітчизняного законодавства та міжнародних стандартів (GDPR, ISO/IEC 27001).

Дисципліна є фаховою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» за освітньою програмою «Організація захисту інформації в інформаційно-комунікаційних системах» та забезпечує формування фахових компетентностей у сфері інформаційної безпеки.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації у сфері захисту даних: виявлення загроз, порівняння методів захисту, формування обґрунтованих висновків щодо ризиків для конфіденційності.

Комунікація

Здатність до фахової комунікації: чітко пояснювати вимоги до захисту даних, аргументовано формулювати рекомендації, оформлювати технічну документацію, звіти та аналітичні матеріали з питань безпеки.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час виконання лабораторних робіт та підготовки проектів із захисту конфіденційних даних.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді при проведенні аудитів безпеки, розробці політик захисту даних та вирішенні комплексних завдань із забезпечення конфіденційності в організаціях.

Студент повинен вміти: аналізувати технічну та нормативну інформацію у сфері захисту даних; виявляти ризики та вразливості; планувати та впроваджувати заходи захисту; документувати результати аналізу; ефективно взаємодіяти з командою.

Фахові компетентності

Розуміння концепцій захисту даних

Розуміння сутності та закономірностей захисту конфіденційних даних в інформаційно-комунікаційних системах. Знання категорій конфіденційності, моделей загроз, принципів мінімізації даних та обмеження доступу відповідно до діючих стандартів.

Аналіз загроз та вразливостей

Здатність аналізувати загрози конфіденційності, виявляти вразливості інформаційних систем, оцінювати ризики витоку даних та обирати адекватні технічні й організаційні контрзаходи для їх мінімізації.

Правове регулювання та стандарти

Знання нормативно-правової бази захисту персональних і конфіденційних даних в Україні та ЄС: Закон «Про захист персональних даних», GDPR, ISO/IEC 27001/27701. Розуміння ролі регуляторів та механізмів відповідальності.

Технічні механізми захисту

Орієнтування в криптографічних методах, механізмах контролю доступу, технологіях анонімізації та псевдонімізації; використання сучасних інструментів для технічного захисту конфіденційних даних в ІКС.

Результати навчання

01

Пояснення ключових понять

Пояснювати сутність ключових понять і категорій: конфіденційність, цілісність, доступність, персональні дані, суб'єкт даних, контролер, обробник, DPIA, DPO, псевдонімізація, анонімізація, витік даних.

02

Характеристика правових механізмів

Характеризувати правові механізми захисту конфіденційних даних, застосовувати методи порівняльного аналізу вітчизняного та міжнародного законодавства, визначати вимоги до обробки та захисту даних.

03

Аналіз загроз та проектування захисту

Аналізувати актуальні загрози конфіденційності, проводити оцінку ризиків (DPIA), проектувати системи захисту конфіденційних даних із урахуванням технічних та організаційних вимог.

04

Практичне застосування інструментів

Застосовувати технічні засоби захисту: криптографічні протоколи, механізми контролю доступу, системи виявлення вторгнень; розробляти та впроваджувати політики конфіденційності для організацій.

МОДУЛЬ 1

Правові та концептуальні основи захисту конфіденційних даних

1 — Тема 1.1

Поняття конфіденційності та конфіденційних даних. Категорії та класифікація даних за ступенем конфіденційності

2 — Тема 1.2

Нормативно-правова база захисту персональних даних в Україні: Закон «Про захист персональних даних», суміжне законодавство

3 — Тема 1.3

Міжнародні стандарти захисту даних: GDPR, ISO/IEC 27001, ISO/IEC 27701. Гармонізація з українським законодавством

4 — Тема 1.4

Організаційно-правовий механізм захисту конфіденційних даних в організації. Ролі контролера, обробника, DPO

МОДУЛЬ 1 · ТЕМА 1.1

Поняття конфіденційності та класифікація даних

Лекційний матеріал (2 год.)

Лекція 1: Поняття «конфіденційна інформація» та «конфіденційні дані»: сутність, відмінності, правовий статус. Тріада CIA (Confidentiality, Integrity, Availability). Класифікація інформації за ступенем конфіденційності: відкрита, службова, конфіденційна, таємна. Категорії персональних даних за Законом України «Про захист персональних даних»: звичайні та особливі категорії.

Принципи обробки конфіденційних даних: законність, справедливість, прозорість; мінімізація даних; обмеження мети; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність (принципи GDPR).

Ключові питання лекції

- Поняття конфіденційності в правовому та технічному вимірах
- Категорії персональних даних та особливості їх обробки
- Тріада CIA як базова концепція інформаційної безпеки
- Принципи обробки даних відповідно до GDPR
- Відповідальність суб'єктів за порушення конфіденційності

Лабораторне заняття (2 год.)

Завдання 1. Класифікація набору тестових даних за ступенем конфіденційності відповідно до вітчизняного законодавства та GDPR. Заповнення матриці класифікації.

Завдання 2. Кейс: аналіз реальних витоків даних в українських організаціях (2022–2024 рр.) — визначення категорій скомпрометованих даних та правових наслідків.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024) — розділ «Концептуальні засади»
- Підготовка реферату: «Категорії персональних даних в українському та європейському праві: порівняльний аналіз»
- Складання схеми «Класифікація конфіденційних даних в ІКС» із прикладами для IT-компанії

Очікуваний результат: студент вміє класифікувати дані за ступенем конфіденційності, застосовувати принципи тріади CIA та орієнтуватися у правових категоріях персональних даних.

МОДУЛЬ 1 · ТЕМА 1.2

Нормативно-правова база захисту персональних даних в Україні

1

Закон «Про захист персональних даних»

№ 2297-VI (2010, зі змінами). Суб'єкти відносин, права суб'єктів даних, обов'язки контролерів.

2

Законопроєкт № 8153

Новий Закон «Про захист персональних даних» (2022). Гармонізація з GDPR, DPO, DPIA, реєстр обробки.

3

Суміжне законодавство

Закони «Про інформацію», «Про кібербезпеку», «Про електронні довірчі послуги», КК України (ст. 182, 361).

4

Регулятор та відповідальність

Уповноважений ВРУ з прав людини. Адміністративна та кримінальна відповідальність за порушення.

Лекційний матеріал (2 год.)

Система законодавства про захист персональних даних в Україні. Закон «Про захист персональних даних» № 2297-VI: структура, основні поняття, права суб'єктів даних. Законопроєкт № 8153 як крок до євроінтеграції. Повноваження Уповноваженого ВРУ з прав людини у сфері захисту персональних даних. Юридична відповідальність за порушення законодавства про конфіденційність.

Лабораторне заняття (2 год.) та СРС (7 год.)

Лабораторна: Аналіз Закону «Про захист персональних даних» № 2297-VI та законопроєкту № 8153 — порівняльна таблиця ключових положень; розбір судових рішень у справах про порушення конфіденційності даних; дискусія «Реформа законодавства: чи готова Україна до повноцінного GDPR?».

СРС: Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024) — розділ «Національно-правова база»; підготовка аналітичної записки «Законопроєкт № 8153: нові вимоги для IT-підприємств України».

МОДУЛЬ 1 · ТЕМИ 1.3–1.4

Міжнародні стандарти та організаційно-правовий механізм захисту

Тема 1.3 — Міжнародні стандарти (Лекція 3, 2 год.)

GDPR (Регламент ЄС 2016/679): сфера застосування, ключові вимоги, права суб'єктів даних. ISO/IEC 27001 — система управління інформаційною безпекою. ISO/IEC 27701 — система управління конфіденційністю. Застосування стандартів до IT-компаній, що працюють з даними громадян ЄС. Сертифікація та аудит відповідності.

Лабораторна (2 год.): Аналіз вимог GDPR щодо обробки персональних даних; порівняння вимог GDPR та Закону України № 2297-VI; кейс «Відповідність IT-компанії вимогам GDPR: що необхідно змінити?».

СРС (7 год.): Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. II» (2024) — розділ «Стандарти безпеки»; підготовка реферату «ISO/IEC 27701 як розширення ISO 27001 для управління конфіденційністю».

Тема 1.4 — Організаційно-правовий механізм (Лекція 4, 2 год.)

Ролі та відповідальність у системі захисту конфіденційних даних: контролер, обробник, уповноважений із захисту даних (DPO). Обов'язки DPO, порядок призначення, незалежність. Договір про обробку персональних даних (DPA). Реєстр операцій обробки (RoPA). Передача даних третім сторонам та за межі ЄС (SCC, BCR). Розробка внутрішньої політики конфіденційності організації.

Лабораторна (2 год.): Розробка структури Politique конфіденційності для умовної IT-компанії; складання реєстру операцій обробки (RoPA); аналіз договору DPA.

СРС (7 год.): Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024); підготовка порівняльної таблиці «Вимоги до DPO за GDPR та законопроєктом № 8153».

МОДУЛЬ 2

Загрози конфіденційності та оцінка ризиків

Тема 2.1

Класифікація загроз конфіденційності даних. Модель порушника. Актуальні вектори атак на конфіденційні дані.

Тема 2.2

Оцінка впливу на захист даних (DPIA). Методологія аналізу ризиків для конфіденційності. Управління інцидентами.

Тема 2.3

Соціальна інженерія та інсайдерські загрози як чинники витоку конфіденційних даних. Методи протидії.

Тема 2.4

Реагування на інциденти з витоком даних (Data Breach). Повідомлення регулятора та суб'єктів даних. Документування.

МОДУЛЬ 2 · ТЕМА 2.1

Загрози конфіденційності та модель порушника

Лекційний матеріал (2 год.)

Класифікація загроз конфіденційності: зовнішні (кіберзлочинці, APT-групи, конкуренти) та внутрішні (інсайдери, помилки персоналу). Модель порушника (threat actor): цілі, можливості, мотивація. Актуальні вектори атак: фішинг, SQL-ін'єкції, атаки на ланцюг постачання, витоки через хмарні сервіси. Аналіз реальних інцидентів в Україні (2022–2024 рр.). Концепція Privacy by Design та Privacy by Default.

Ключові питання

- Класифікація загроз конфіденційності за ENISA та ДССЗЗІ
- Модель порушника: типи, можливості, вектори атак
- Фішинг і соціальна інженерія як основні причини витоків
- Загрози конфіденційності в хмарних середовищах
- Принципи Privacy by Design у розробці ІКС

Лабораторне заняття (2 год.)

Завдання 1. Побудова моделі загроз для умовної ІКС: визначення активів, загроз, вразливостей та потенційних порушників за методологією STRIDE.

Завдання 2. Кейс: аналіз реального кіберінциденту з витоком конфіденційних даних — визначення вектора атаки, скомпрометованих даних, наслідків та рекомендацій.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. І» (2024) — розділ «Загрози та вразливості»
- Підготовка реферату: «APT-атаки на українські організації 2022–2024 рр.: аналіз векторів витоку конфіденційних даних»
- Складання класифікаційної таблиці загроз конфіденційності за критеріями DREAD

Очікуваний результат: студент вміє будувати модель загроз, класифікувати вектори атак на конфіденційні дані та застосовувати принципи Privacy by Design.

МОДУЛЬ 2 · ТЕМА 2.2

Оцінка впливу на захист даних (DPIA) та управління ризиками

Крок 1

Визначення необхідності DPIA. Скринінг операцій обробки за критеріями ризику.

Крок 2

Опис операцій обробки: цілі, категорії даних, суб'єкти, одержувачі.

Крок 3

Оцінка необхідності та пропорційності. Аналіз відповідності принципам захисту даних.

Крок 4

Ідентифікація та оцінка ризиків для прав і свобод суб'єктів даних.

Крок 5

Заходи з управління ризиками. Схвалення DPO. Документування та перегляд DPIA.

Лекційний матеріал (2 год.)

Data Protection Impact Assessment (DPIA): призначення, правова основа (ст. 35 GDPR), випадки обов'язкового проведення. Методологія DPIA: кроки, учасники, документація. Реєстр ризиків конфіденційності. Управління ризиками за ISO/IEC 27005. Зв'язок DPIA з процесом управління змінами в ІКС.

Лабораторне заняття (2 год.) та СРС (7 год.)

Лабораторна: Проведення DPIA для умовного проєкту з обробки персональних даних (медична система / HR-платформа); заповнення шаблону DPIA; визначення заходів пом'якшення ризиків.

СРС: Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024) — розділ «DPIA та управління ризиками»; підготовка аналітичної записки «DPIA як інструмент Privacy by Design: практика ЄС та перспективи для України».

МОДУЛЬ 2 · ТЕМИ 2.3–2.4

Соціальна інженерія, інсайдерські загрози та реагування на інциденти

Тема 2.3 — Соціальна інженерія та інсайдери (Лекція 7, 2 год.)

Соціальна інженерія як основний вектор витоку конфіденційних даних: фішинг, вішинг, претекстинг, бейтинг. Інсайдерські загрози: типи інсайдерів (зловмисний, необережний, скомпрометований), мотивація, індикатори. Технічні засоби виявлення інсайдерів: DLP-системи, UEBA, моніторинг активності. Організаційні заходи: навчання персоналу, NDA, розподіл привілеїв, принцип найменших прав.

Лабораторна (2 год.): Налаштування правил DLP-системи для захисту конфіденційних даних; аналіз журналів аномальної активності; кейс «Інсайдерський витік даних: виявлення та реагування».

СРС (7 год.): Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. II» (2024) — розділ «Соціотехнічні атаки та DLP»; підготовка реферату «Програма підвищення обізнаності персоналу щодо захисту конфіденційних даних».

Тема 2.4 — Реагування на витоки даних (Лекція 8, 2 год.)

Data Breach: визначення, типи, правові наслідки. Процедура реагування на витік даних (Incident Response): виявлення, локалізація, ліквідація, відновлення, аналіз. Вимоги GDPR щодо повідомлення регулятора (72 год.) та суб'єктів даних. Документування інцидентів: журнал порушень, звіт про інцидент. Forensic-аналіз у контексті захисту конфіденційних даних. Уроки з реальних витоків даних в Україні (2022–2024 рр.).

Лабораторна (2 год.): Розробка плану реагування на інцидент витоку конфіденційних даних для умовної організації; складання повідомлення регулятору та суб'єктам даних.

СРС (7 год.): Підготовка аналітичної записки «Реагування на кіберінциденти з витоком конфіденційних даних в Україні: кращі практики та правові вимоги».

МОДУЛЬ 3

Технічні методи та засоби захисту конфіденційних даних

Тема 3.1

Криптографічні методи захисту конфіденційних даних: симетричне та асиметричне шифрування, хешування, ЕЦП.

Тема 3.2

Контроль доступу до конфіденційних даних: моделі управління доступом (RBAC, ABAC, MAC, DAC). Автентифікація.

Тема 3.3

Анонімізація та псевдонімізація даних. Диференційна приватність. Методи захисту даних при обробці та передачі.

Тема 3.4

Захист конфіденційних даних у хмарних середовищах та при використанні Big Data і штучного інтелекту.

МОДУЛЬ 3 · ТЕМА 3.1

Криптографічні методи захисту конфіденційних даних

Лекційний матеріал (2 год.)

Криптографія як основа технічного захисту конфіденційності. Симетричне шифрування: AES-256, блокові та потокові шифри, режими роботи (CBC, GCM). Асиметричне шифрування: RSA, ECC — принципи, застосування, управління ключами. Криптографічні хеш-функції: SHA-256, SHA-3 — цілісність та автентифікація даних. Електронний цифровий підпис (ЕЦП) в Україні: правова база, кваліфікований ЕП. Шифрування на рівні сховища (at rest) та каналу передачі (in transit): TLS/SSL, VPN, IPsec. Управління ключами: PKI, HSM.

Ключові питання

- Симетричне та асиметричне шифрування: порівняння та сфери застосування
- AES-256 як стандарт захисту конфіденційних даних
- Управління ключами шифрування: PKI та HSM
- TLS 1.3 як протокол захисту даних при передачі
- Правова база електронного цифрового підпису в Україні

Лабораторне заняття (2 год.)

Завдання 1. Практичне шифрування конфіденційних файлів із використанням AES-256 (OpenSSL/Python): генерація ключів, шифрування, дешифрування, верифікація цілісності.

Завдання 2. Налаштування TLS-з'єднання для захищеної передачі конфіденційних даних: аналіз сертифіката, перевірка ланцюга довіри, виявлення вразливостей конфігурації.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. І» (2024) — розділ «Криптографічні методи»
- Підготовка реферату: «Квантова криптографія та постквантові алгоритми: виклики для захисту конфіденційних даних»
- Аналіз сучасних стандартів шифрування ДСТУ для захисту конфіденційної інформації

Очікуваний результат: студент вміє застосовувати криптографічні методи для захисту конфіденційних даних та налаштовувати шифрування на різних рівнях ІКС.

МОДУЛЬ 3 · ТЕМА 3.2

Контроль доступу до конфіденційних даних

Лекційний матеріал (2 год.)

Концепція контролю доступу як основи захисту конфіденційності. Моделі управління доступом: DAC (дискреційна), MAC (мандатна), RBAC (рольова), ABAC (атрибутивна). Принцип найменших привілеїв (PoLP) та розподіл обов'язків (SoD). Сучасні рішення IAM (Identity and Access Management): LDAP, Active Directory, Zero Trust Architecture. Багатофакторна автентифікація (MFA): TOTP, FIDO2, апаратні токени. Журналювання та аудит доступу до конфіденційних даних. Управління привілейованим доступом (PAM).

Лабораторне заняття (2 год.) та СРС (7 год.)

Лабораторна: Налаштування рольової моделі доступу (RBAC) для умовної системи обробки конфіденційних даних; конфігурація MFA; аналіз журналів аудиту доступу; виявлення аномалій; кейс «Zero Trust для захисту конфіденційних даних IT-компанії».

СРС: Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. II» (2024) — розділ «Управління доступом»; підготовка аналітичної записки «Zero Trust Architecture: принципи та впровадження для захисту конфіденційних даних».

Очікуваний результат: студент вміє проектувати та налаштовувати системи контролю доступу, застосовувати принцип PoLP та конфігурувати MFA для захисту конфіденційних даних.

МОДУЛЬ 3 · ТЕМА 3.3

Анонімізація, псевдонімізація та приватність даних

Анонімізація

Незворотне перетворення даних: узагальнення, приховування, збурення, агрегування. Оцінка ризику де-анонімізації.

Псевдонімізація

Зворотне перетворення: заміна ідентифікаторів псевдонімами. Збереження окремо ключа відповідності. Вимоги GDPR.

Диференційна приватність

Математичний гарантований захист приватності при аналізі даних. Застосування в Big Data та ML-системах.

Лекційний матеріал (2 год.)

Анонімізація та псевдонімізація у контексті GDPR: правова кваліфікація, вимоги та обмеження. Методи анонімізації: k-анонімність, l-різноманітність, t-близькість. Ризик де-анонімізації: проблема повторної ідентифікації. Диференційна приватність: концепція ε-DP, механізми Лапласа та Гаусса. Захист конфіденційних даних при їх публікації та передачі для аналізу. Технологія Privacy Enhancing Technologies (PET).

Лабораторне заняття (2 год.) та СРС (7 год.)

Лабораторна: Практична анонімізація датасету з персональними даними (Python/ARX): застосування k-анонімності, оцінка якості анонімізації та ризику де-анонімізації; порівняння методів анонімізації за критеріями корисності та конфіденційності.

СРС: Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024) — розділ «PET та анонімізація»; підготовка реферату «Методи анонімізації даних у системах охорони здоров'я: виклики та рішення».

МОДУЛЬ 3 · ТЕМА 3.4

Захист конфіденційних даних у хмарних середовищах та Big Data

Лекційний матеріал (2 год.)

Специфіка захисту конфіденційних даних у хмарних середовищах: моделі розгортання (IaaS, PaaS, SaaS), модель спільної відповідальності. Основні загрози хмарній конфіденційності: несанкціонований доступ, витоки через API, мультиорендність. Технічні рішення: Cloud Access Security Broker (CASB), шифрування на стороні клієнта (BYOK). Конфіденційність у Big Data: проблеми агрегації, re-identification, великомасштабного профілювання. Privacy в ML/AI: атаки на навчальні моделі (model inversion, membership inference). Технологія Federated Learning для захисту конфіденційності.

Ключові питання

- Модель спільної відповідальності за безпеку в хмарі
- CASB як інструмент захисту конфіденційних даних у SaaS
- Ризики конфіденційності у Big Data та ML-системах
- Federated Learning як Privacy-preserving підхід
- Відповідальність за конфіденційність при передачі даних хмарному провайдеру

Лабораторне заняття (2 год.)

Завдання 1. Аналіз політики безпеки та конфіденційності провідних хмарних провайдерів (AWS, Azure, Google Cloud) щодо захисту персональних даних: відповідність вимогам GDPR та законодавству України.

Завдання 2. Кейс: проектування захисту конфіденційних даних для умовної хмарної системи — вибір механізмів шифрування, контролю доступу та моніторингу.

Завдання 3. Дискусія: «Хмарні сервіси іноземних провайдерів для обробки конфіденційних даних громадян України: ризики та допустимість».

Самостійна робота (7 год.)

- Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. II» (2024) — розділ «Хмарна безпека»
- Підготовка аналітичної записки «Захист персональних даних у хмарних сервісах: вимоги GDPR та законодавства України»
- Складання таблиці «Механізми захисту конфіденційних даних у хмарних моделях IaaS/PaaS/SaaS»

Очікуваний результат: студент вміє оцінювати ризики конфіденційності у хмарних середовищах та Big Data, застосовувати відповідні технічні та організаційні заходи захисту.

МОДУЛЬ 4

Організаційні заходи та практика захисту конфіденційних даних

Тема 4.1

Система управління захистом конфіденційних даних в організації. Політики, процедури, стандарти. Аудит безпеки.

Тема 4.2

Захист конфіденційних даних при розробці програмного забезпечення. Принципи Secure by Design, DevSecOps.

Тема 4.3

Конфіденційність у корпоративному середовищі: BYOD, хмарна праця, дистанційна робота. DLP-системи та SIEM.

Тема 4.4

Сучасні виклики захисту конфіденційних даних: штучний інтелект, IoT, блокчейн, воєнний стан та кіберзахист.

МОДУЛЬ 4 · ТЕМА 4.1

Система управління захистом конфіденційних даних в організації

Лекційний матеріал (2 год.)

Система управління інформаційною безпекою (ISMS) за ISO/IEC 27001: структура, цикл PDCA, сфера застосування. Розробка та впровадження документації: Політика конфіденційності, Процедура обробки персональних даних, NDA, Угода про конфіденційність. Аудит захисту конфіденційних даних: внутрішній та зовнішній. Gap-аналіз відповідності вимогам GDPR/ISO 27001. Метрики ефективності ISMS. Управління постачальниками та підрядниками як ризик конфіденційності.

Ключові питання

- Структура ISMS за ISO/IEC 27001 та ISO/IEC 27701
- Ключові документи системи управління конфіденційністю
- Методологія внутрішнього аудиту захисту даних
- Gap-аналіз відповідності вимогам GDPR
- Управління ризиками третіх сторін у ланцюгу обробки даних

Лабораторне заняття (2 год.)

Завдання 1. Проведення Gap-аналізу відповідності умовної організації вимогам GDPR: визначення відповідностей, невідповідностей та рекомендацій.

Завдання 2. Розробка пакету внутрішньої документації: Політика конфіденційності, Процедура реагування на запити суб'єктів даних.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024) — розділ «Організаційні заходи»
- Підготовка реферату: «Впровадження ISO/IEC 27701 в українських IT-компаніях: переваги та виклики»
- Складання чек-листу аудиту відповідності вимогам GDPR для IT-підприємства

Очікуваний результат: студент вміє проводити Gap-аналіз, розробляти внутрішню документацію з захисту конфіденційних даних та планувати заходи з підвищення відповідності стандартам.

МОДУЛЬ 4 · ТЕМА 4.2

Захист конфіденційних даних при розробці ПЗ (Secure SDLC)

Лекційний матеріал (2 год.)

Концепція Privacy by Design та Security by Design у розробці ПЗ. Принципи Secure SDLC: вбудування безпеки на кожному етапі (вимоги, дизайн, код, тестування, деплой). Огляд загроз за методологією OWASP Top 10 у контексті конфіденційності даних. SAST та DAST: автоматизований аналіз коду на вразливості. Безпечне зберігання конфіденційних даних у базах даних: шифрування, хешування паролів (bcrypt, Argon2). DevSecOps: інтеграція перевірок безпеки у CI/CD-конвеєр.

Лабораторне заняття (2 год.) та СРС (7 год.)

Лабораторна: Аналіз вразливостей зразка вихідного коду веб-застосунку (OWASP WebGoat/DVWA) — ідентифікація ризиків конфіденційності, виправлення вразливостей; реалізація безпечного зберігання паролів та конфіденційних даних у БД.

СРС: Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. II» (2024) — розділ «Безпека застосунків»; підготовка аналітичної записки «Privacy by Design у розробці мобільних застосунків: вимоги GDPR та практичні рішення».

Очікуваний результат: студент вміє застосовувати принципи Secure SDLC, виявляти та усувати вразливості, що загрожують конфіденційності даних у програмних системах.

МОДУЛЬ 4 · ТЕМА 4.3

Конфіденційність у корпоративному середовищі: DLP та SIEM

Лекційний матеріал (2 год.)

Захист конфіденційних даних у сучасному корпоративному середовищі: BYOD-політика, дистанційна робота, хмарна співпраця. Data Loss Prevention (DLP): архітектура, типи (мережевий, кінцевих точок, хмарний), правила виявлення. SIEM-системи (Security Information and Event Management): збір логів, кореляція подій, виявлення аномалій у доступі до конфіденційних даних. UEBA (User and Entity Behavior Analytics) для захисту від інсайдерських витоків. Моніторинг дотримання політик конфіденційності.

Лабораторне заняття (2 год.) та СРС (7 год.)

Лабораторна: Налаштування правил DLP для захисту конфіденційних даних (Email, USB, Cloud); аналіз подій SIEM для виявлення потенційного витоку конфіденційних даних; розробка BYOD-політики для умовної організації.

СРС: Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах. Ч. І» (2024) — розділ «DLP та SIEM»; підготовка аналітичної записки «DLP-системи в умовах дистанційної роботи: ефективність та правові обмеження».

Очікуваний результат: студент вміє налаштовувати та застосовувати DLP-системи та SIEM для захисту конфіденційних даних і моніторингу їх обробки в корпоративному середовищі.

МОДУЛЬ 4 · ТЕМА 4.4

Сучасні виклики захисту конфіденційних даних

Лекційний матеріал (2 год.)

Штучний інтелект та конфіденційність: автоматизовані рішення (ст. 22 GDPR), профілювання, explainable AI. IoT та конфіденційність: особливості збору даних, мінімізація, безпека комунікацій. Блокчейн та конфіденційність: незмінність vs. право на забуття (ст. 17 GDPR). Захист конфіденційних даних в умовах воєнного стану: кіберзагрози, атаки на критичну інфраструктуру, захист державних реєстрів. Роль ДССЗЗІ, CERT-UA у захисті конфіденційних даних. Перспективи: квантова криптографія, Privacy-preserving Computing.

Ключові питання

- Правові вимоги до автоматизованих рішень та профілювання за GDPR
- IoT як новий вектор загроз конфіденційності
- Право на забуття та технічна незмінність блокчейну
- Кіберзагрози конфіденційним даним в умовах воєнного стану
- Квантова загроза сучасній криптографії та постквантовий захист

Лабораторне заняття (2 год.)

Завдання 1. Аналіз відповідності AI-системи вимогам конфіденційності: оцінка ризиків профілювання та автоматизованого прийняття рішень за GDPR.

Завдання 2. Дискусія: «Захист конфіденційних даних громадян України в умовах повномасштабної кібервійни: виклики та відповіді ДССЗЗІ та CERT-UA».

Завдання 3. Підготовка та презентація міні-проекту: «Розробка стратегії захисту конфіденційних даних для умовної організації — комплексний підхід».

Самостійна робота (7 год.)

- Опрацювання: Думчиков М. О. та ін. «Захист персональних даних у кіберпросторі» (2024) — розділ «Сучасні виклики»
- Підготовка аналітичної записки «Захист конфіденційних даних в системах штучного інтелекту: вимоги AI Act та GDPR»
- Аналіз звітів CERT-UA про кіберінциденти з витоком конфіденційних даних (2022–2024 рр.)

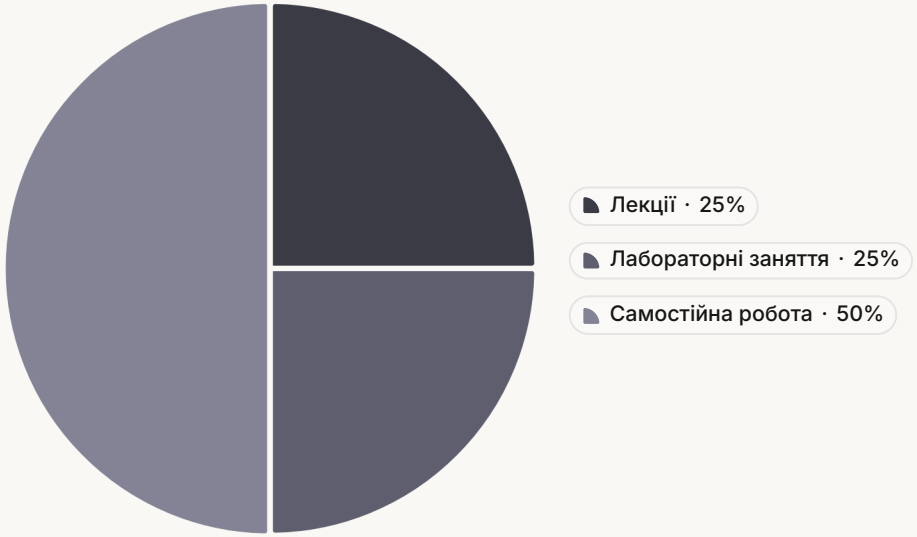
Очікуваний результат: студент вміє аналізувати нові виклики конфіденційності даних, оцінювати ризики у контексті AI, IoT та блокчейн, розробляти комплексні стратегії захисту.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Поняття конфіденційності, класифікація	2	2	7
	Тема 1.2 — Нормативно-правова база України	2	2	7
	Тема 1.3 — GDPR, ISO/IEC 27001, 27701	2	2	7
	Тема 1.4 — Ролі контролера, обробника, DPO	2	2	7
Модуль 2	Тема 2.1 — Загрози, модель порушника	2	2	7
	Тема 2.2 — DPIA та управління ризиками	2	2	7
	Тема 2.3 — Соціальна інженерія та інсайдери	2	2	7
	Тема 2.4 — Реагування на Data Breach	2	2	7
Модуль 3	Тема 3.1 — Криптографічні методи захисту	2	2	7
	Тема 3.2 — Контроль доступу (RBAC, MFA, ZTA)	2	2	7
	Тема 3.3 — Анонімізація, псевдонімізація, PET	2	2	7
	Тема 3.4 — Захист у хмарних середовищах та Big Data	2	2	7
Модуль 4	Тема 4.1 — ISMS, аудит, документація	2	2	7
	Тема 4.2 — Secure SDLC, Privacy by Design	2	2	7
	Тема 4.3 — DLP, SIEM, корпоративне середовище	2	2	7
	Тема 4.4 — AI, IoT, блокчейн, виклики сучасності	2	2	7
Разом	**16 тем**	**30**	**30**	**60**

Загальний обсяг: 120 годин = 4 кредити ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **120 годин (4 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теоретичними знаннями та практичними навичками захисту конфіденційних даних.

Лекції — 30 год. (25%)

Системне подання ключового теоретичного матеріалу: правова база, концепції захисту даних, технічні методи та організаційні заходи з використанням схем, таблиць і практичних прикладів.

Лабораторні — 30 год. (25%)

Практичне відпрацювання навичок: налаштування систем захисту, проведення DPIA, розробка документації, аналіз інцидентів, робота з інструментами криптографії та DLP.

Самостійна робота — 60 год. (50%)

Поглиблене вивчення, підготовка аналітичних матеріалів, 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 конфіденційних даних (Думчиков, Костюк, Складанний та ін.), нормативно-правовими актами (GDPR, Закон № 2297-VI), стандартами ISO/IEC 27001/27701 та науковими статтями у фахових виданнях. Студент конспектує ключові положення та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (порівняльний аналіз стандартів і законодавства, оцінка відповідності вимогам GDPR, аналіз інцидентів); творчих завдань — аналітичні записки, реферати, міні-дослідження з актуальних питань захисту конфіденційних даних в ІКС.

Робота з інформаційними ресурсами

Опрацювання офіційних ресурсів: ДССЗЗІ (**dsszzi.gov.ua**), CERT-UA (**cert.gov.ua**), Уповноважений ВРУ з прав людини (**ombudsman.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**). Аналіз звітів про кіберінциденти, ENISA, OWASP.

Підготовка до занять

Підготовка до лабораторних занять (опрацювання інструментів, вивчення методологій DPIA, STRIDE, OWASP); підготовка до тестувань (терміни, стандарти, вимоги); підготовка до контрольних робіт за кожним модулем (систематизація знань).

Форми контролю знань

1	2	3
Поточний контроль	Проміжний контроль	Підсумковий контроль
Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання лабораторних робіт, якість звітів і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Проводиться після кожної теми у формі тестування (10–15 питань) або усного захисту лабораторної роботи.	Самостійна робота — комплексне практичне завдання або аналітична записка, які охоплюють теми змістовних модулів (правові вимоги, технічні рішення, організаційні заходи). Оцінюються повнота відповіді, аргументованість та обґрунтованість рекомендацій. Проводиться після завершення кожного змістовного модуля.	Залік або іспит відповідно до навчального плану. Форма проведення — тестування та практичне завдання (розробка моделі захисту конфіденційних даних). Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Захист конфіденційних даних» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок у сфері захисту конфіденційних даних, необхідних для майбутньої фахової діяльності у галузі комп'ютерної інженерії та інформаційної безпеки.

Лекції

Системне подання теоретичного матеріалу з використанням схем, таблиць і прикладів реальних кіберінцидентів; студенти ведуть конспекти та задають уточнювальні запитання.

Робота з нормативною базою

Опрацювання GDPR, ISO-стандартів, законодавства України; формування навичок аналізу вимог та їх практичного застосування до конкретних систем обробки даних.

Кейс-стаді

Аналіз реальних інцидентів витоку конфіденційних даних в Україні та світі; студенти визначають вектор атаки, правові наслідки та рекомендації із захисту.

Дискусії

Обговорення дискусійних питань: GDPR vs. вітчизняне законодавство, баланс приватності та безпеки, захист даних в умовах воєнного стану; розвиток критичного мислення.

Лабораторні дослідження

Практична робота з інструментами: OpenSSL, Python-криптографія, DLP-системи, SIEM, ARX (анонімізація); відпрацювання реальних сценаріїв захисту конфіденційних даних.

Проектна робота

Розробка комплексного проекту захисту конфіденційних даних для умовної організації: від моделі загроз до політики конфіденційності та плану реагування на інциденти.

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

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

1. Думчиков М. О. та ін.

Захист персональних даних у кіберпросторі : навч. посіб. / М. О. Думчиков, О. С. Малетова, М. С. Уткіна, В. К. Ободяк. — Суми : СумДУ, 2024. — 245 с. (проєкт ERASMUS+ Jean Monnet «EUEPPDC»).

2. Костюк Ю. В., Складанний П. М.

Захист інформації в комп'ютерних системах та мережах. Частина I : підручник. — Київ : Київський університет імені Бориса Грінченка, 2024. — 352 с.

3. Костюк Ю. В., Складанний П. М.

Захист інформації в комп'ютерних системах та мережах. Частина II : підручник. — Київ : Київський університет імені Бориса Грінченка, 2024. — 386 с.

4. Прокофьєв М. І., Половенко Л. П., Гресь О. В.

Кібербезпека та захист інформації : навч. посіб. для бакалаврів спеціальності 125. — Вінниця : ДонНУ імені Василя Стуса, 2023. — 198 с.

5. Рибальченко О. В., Мусієнко А. П.

Інформаційна безпека та захист персональних даних в умовах цифрової трансформації : монографія. — Київ : КНЕУ, 2023. — 264 с.

6. Петров В. В., Коваль Т. І.

Організаційно-технічні заходи захисту конфіденційної інформації в ІКС : навч. посіб. — Харків : ХНУРЕ, 2022. — 220 с.

7. Грищук Р. В., Даник Ю. Г.

Основи кібербезпеки : підручник. — 2-ге вид., оновл. — Житомир : ЖНАЕУ, 2022. — 636 с.

8. Хорошко В. О. та ін.

Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало та ін. — Львів : Вид-во Львівської політехніки, 2022. — 320 с.

Додаткова література та наукові статті

9. Бурячок В. Л. та ін.

Соціальна та комплексна інженерія в кібербезпеці : навч. посіб. — Київ : ПВП «Задруга», 2023. — 288 с. *Рекомендується для тем 2.1–2.3 (загрози та соціальна інженерія).*

10. Андреєв О. В., Кузьменко І. М.

Захист персональних даних в умовах воєнного стану та кіберпростору. Юридичний науковий електронний журнал. — 2023. — № 4. — С. 112–119. *Рекомендується для тем 4.4.*

11. Марущак А. І., Довгань О. Д.

Правовий режим конфіденційної інформації в Україні: сучасний стан та перспективи гармонізації з правом ЄС. — Київ : НА СБ України, 2022. — 196 с. *Рекомендується для модуля 1.*

12. Ніколаєнко С. М., Семенченко А. І.

Управління кіберінцидентами та захист критичної інфраструктури : навч. посіб. — Київ : НАДУ, 2023. — 312 с. *Рекомендується для тем 2.4, 4.3.*

Нормативно-правова база

- Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010

  Основний закон, що регулює обробку та захист персональних даних в Україні. **zakon.rada.gov.ua**

- Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017

  Визначає правові та організаційні основи забезпечення кібербезпеки держави. **zakon.rada.gov.ua**

- Закон України «Про електронні довірчі послуги» № 2155-VIII від 05.10.2017

  Регулює надання електронних довірчих послуг, у т.ч. кваліфікованого ЕП. **zakon.rada.gov.ua**

- Регламент ЄС 2016/679 (GDPR) — Загальний регламент про захист даних

  Ключовий міжнародний нормативний акт у сфері захисту персональних даних, обов'язковий для компаній, що обробляють дані громадян ЄС. **gdpr-text.com**

- Стандарти ДСТУ ISO/IEC 27001:2023 та ДСТУ ISO/IEC 27701:2022

  Національні стандарти систем управління інформаційною безпекою та конфіденційністю. **uas.org.ua**

Офіційні ресурси та фахові видання

ДССЗЗІ України

dsszzi.gov.ua — Державна служба спеціального зв'язку та захисту інформації: нормативна база, стандарти, методичні матеріали з технічного захисту інформації.

CERT-UA

cert.gov.ua — Урядова команда реагування на кіберінциденти: звіти про кіберзагрози, рекомендації, аналіз актуальних атак на конфіденційні дані.

Уповноважений ВРУ з прав людини

ombudsman.gov.ua — регулятор у сфері захисту персональних даних в Україні: роз'яснення, рішення, методичні матеріали.

Верховна Рада України

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

Журнал «Захист інформації»

НАУ — провідне фахове видання з питань технічного та організаційного захисту інформації в Україні.

ENISA — Агентство ЄС з кібербезпеки

enisa.europa.eu — звіти про загрози, настанови з конфіденційності, рекомендації з GDPR-відповідності.

OWASP Foundation

owasp.org — методологія виявлення вразливостей у застосунках (OWASP Top 10), матеріали з Privacy by Design.

Міністерство цифрової трансформації

diia.gov.ua — цифрові послуги держави, матеріали з кібербезпеки та захисту персональних даних громадян України.

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

Чому «Захист конфіденційних даних» для інженерів?

Дисципліна є ключовою фаховою складовою підготовки бакалаврів за ОП «Організація захисту інформації в ІКС». Сучасний інженер комп'ютерних систем несе відповідальність за безпеку та конфіденційність даних, що обробляються у розроблених ним системах.

Розуміння вимог GDPR, ISO/IEC 27001 та вітчизняного законодавства є конкурентною перевагою для українських IT-фахівців, що працюють з міжнародними замовниками та будують глобальні цифрові продукти.

Практичне значення для майбутньої кар'єри

- Розуміння вимог GDPR для роботи з міжнародними IT-замовниками та клієнтами з ЄС
- Навички проектування систем з урахуванням Privacy by Design та Secure SDLC
- Здатність проводити DPIA та Gap-аналіз відповідності ISO 27001 для роботодавців
- Знання технічних засобів захисту (криптографія, DLP, IAM) — ключових для IT-безпеки
- Розуміння правової відповідальності за витік конфіденційних даних у продуктах
- Навички реагування на кіберінциденти та управління Data Breach відповідно до законодавства

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові аспекти захисту конфіденційних даних — від правових засад і моделей загроз до технічних механізмів і організаційних заходів — та формує у студентів цілісну компетентність у сфері забезпечення конфіденційності в інформаційно-комунікаційних системах.

Бажаємо успіхів у вивченні «Захисту конфіденційних даних»!

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

16

Тем

У 4 змістовних модулях

12

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Приватність — це не про те, що приховати. Це про те, що захистити.» — принцип Privacy by Design

Спеціальність 123 · Комп'ютерна інженерія · Бакалавр · ОП «Організація захисту інформації в ІКС» · 4 кредити ЄКТС