Робоча програма дисципліни «Захист інформації в комп'ютерних системах»

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 інформації в комп'ютерних системах

Спеціальність: 123 Комп'ютерна інженерія

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки

Лекції: 30 год. | **Лабораторні:** 30 год. | **СРС:** 60 год.

Призначення дисципліни

Дисципліна «Захист інформації в комп'ютерних системах» формує у студентів системне розуміння принципів, методів та технологій захисту інформації в сучасних комп'ютерних системах і мережах. Курс охоплює теоретичні основи інформаційної безпеки, криптографічні механізми, методи виявлення та протидії кіберзагрозам, нормативно-правову базу у сфері захисту інформації.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» та забезпечує формування фахових компетентностей, передбачених освітньо-професійною програмою.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації у сфері інформаційної безпеки: виявлення вразливостей, порівняння альтернативних методів захисту, формування обґрунтованих рішень.

Комунікація

Здатність до усної та письмової комунікації: чітко пояснювати концепції захисту інформації, аргументовано обстоювати обрані рішення, оформлювати технічні звіти та аналітичні записки.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки лабораторних звітів та індивідуальних досліджень.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групового аналізу інцидентів безпеки, розробки політик захисту та спільного вирішення практичних задач.

Студент повинен вміти: аналізувати загрози та вразливості інформаційних систем; обирати та обґрунтовувати засоби захисту; планувати власну діяльність і дотримуватися дедлайнів; коректно спілкуватися з викладачами та одногрупниками; брати участь у командній роботі та розподіляти обов'язки.

Фахові компетентності

Основи інформаційної безпеки

Розуміння сутності та закономірностей захисту інформації в комп'ютерних системах: конфіденційність, цілісність, доступність. Знання класифікації загроз, моделей порушників та методів оцінки ризиків.

Криптографічний захист

Здатність застосовувати симетричні та асиметричні криптографічні алгоритми, електронний цифровий підпис, хеш-функції та протоколи криптографічного захисту відповідно до національних і міжнародних стандартів.

Захист мереж та систем

Знання методів і засобів захисту комп'ютерних мереж: міжмережеве екранування, системи виявлення вторгнень, VPN, протоколи безпеки. Розуміння особливостей захисту хмарних і бездротових систем.

Нормативно-правова база

Орієнтування в нормативно-правовій базі у сфері захисту інформації в Україні: закони, стандарти, керівні нормативні документи з технічного захисту інформації (НД ТЗІ), міжнародні стандарти серії ISO/IEC 27000.

Результати навчання

01

Пояснення основних понять

Пояснювати сутність ключових понять і явищ: загроза, вразливість, ризик, несанкціонований доступ, конфіденційність, цілісність, доступність, криптографія, автентифікація, авторизація.

02

Характеристика методів захисту

Характеризувати основні методи та механізми захисту інформації: криптографічні, програмно-апаратні, організаційні; застосовувати порівняльний аналіз для вибору оптимального рішення.

03

Аналіз загроз та інцидентів

Аналізувати кіберзагрози, вразливості та інциденти безпеки з метою виявлення їх джерел, механізмів реалізації та наслідків для комп'ютерних систем і мереж.

04

Застосування засобів захисту

Застосовувати криптографічні алгоритми, програмні засоби захисту та налаштовувати базові механізми безпеки комп'ютерних систем відповідно до чинних нормативних вимог.

МОДУЛЬ 1

Теоретичні основи захисту інформації

1

Тема 1.1

Основні поняття інформаційної безпеки. Класифікація загроз і вразливостей. Моделі порушників.

2

Тема 1.2

Нормативно-правова база захисту інформації в Україні. Міжнародні стандарти ISO/IEC 27000.

3

Тема 1.3

Моделі безпеки та політики захисту інформації. Управління ризиками інформаційної безпеки.

4

Тема 1.4

Методи оцінювання захищеності комп'ютерних систем. Аудит інформаційної безпеки.

МОДУЛЬ 1 · ТЕМА 1.1

Основні поняття інформаційної безпеки. Загрози та вразливості.

Лекційний матеріал (2 год.)

Лекція 1: Поняття інформаційної безпеки: конфіденційність, цілісність, доступність (тріада CIA). Інформація як об'єкт захисту. Класифікація інформації за режимом доступу. Поняття загрози, вразливості, ризику, атаки. Категорії загроз: перехоплення, модифікація, відмова в обслуговуванні, несанкціонований доступ.

Моделі порушників: класифікація за мотивами та можливостями. Внутрішні та зовнішні порушники. Антропогенні, техногенні та природні загрози. Статистика кіберінцидентів в Україні та світі. Базові принципи побудови системи захисту інформації.

Ключові питання лекції

- Тріада CIA та її практичне значення для захисту систем
- Класифікація загроз та вразливостей інформаційних систем
- Моделі порушників та їхні можливості
- Принципи мінімальних привілеїв, глибокого захисту та відкритого проектування
- Основні категорії засобів захисту інформації

Лабораторне заняття (2 год.)

Завдання 1. Аналіз реальних кіберінцидентів: побудова таблиці загроз за критеріями (тип загрози, джерело, механізм реалізації, наслідки, засоби протидії).

Завдання 2. Практичне завдання: оцінювання ризиків для модельної інформаційної системи — визначення активів, загроз, вразливостей та розрахунок рівня ризику.

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

Самостійна робота (7 год.)

- Опрацювання посібника: Терейковський І. А., Гнатюк С. О. «Захист інформації в комп'ютерних системах» — розділ «Основи ІБ»
- Підготовка реферату: «Сучасний стан кіберзагроз в Україні: аналіз звітів CERT-UA»
- Складання схеми «Класифікація загроз інформаційної безпеки» з прикладами реальних атак

Очікуваний результат: студент вміє характеризувати основні поняття інформаційної безпеки, класифікувати загрози та вразливості, описувати моделі порушників.

МОДУЛЬ 1 · ТЕМА 1.2

Нормативно-правова база захисту інформації

1

Законодавство України

Закони про захист інформації, кібербезпеку, персональні дані. НД ТЗІ серія.

2

Міжнародні стандарти

ISO/IEC 27001, 27002, 27005. Серія стандартів управління інформаційною безпекою.

3

Регуляторні органи

ДССЗІ, CERT-UA, Держспецзв'язку. Ролі та повноваження у сфері кібербезпеки.

4

Відповідальність

Юридична відповідальність за порушення вимог ІБ. Кримінальний кодекс України.

Лекційний матеріал (2 год.)

Правові основи захисту інформації в Україні: Закон «Про захист інформації в інформаційно-телекомунікаційних системах», Закон «Про кібербезпеку», Закон «Про захист персональних даних». Керівні нормативні документи з технічного захисту інформації (НД ТЗІ). Міжнародні стандарти серії ISO/IEC 27000: структура, вимоги, застосування. Регуляторні органи у сфері кібербезпеки України. Юридична відповідальність за кіберзлочини.

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

Лабораторна: Аналіз вимог стандарту ISO/IEC 27001 до системи управління інформаційною безпекою; порівняння вимог НД ТЗІ з міжнародними стандартами; складання переліку нормативних вимог для конкретного класу ІС.

СРС: Опрацювання: Вишняков В. М. «Захист інформації в комп'ютерних системах» (КНУБА, 2022) — розділ «Нормативна база»; підготовка аналітичної записки «Стратегія кібербезпеки України: аналіз та перспективи».

МОДУЛЬ 1 · ТЕМИ 1.3–1.4

Моделі безпеки, управління ризиками та аудит

Тема 1.3 — Моделі безпеки та управління ризиками (Лекція 3, 2 год.)

Моделі безпеки: дискреційна (DAC), мандатна (MAC), рольова (RBAC). Модель Белла–ЛаПадули, модель Біба. Політика безпеки: поняття, структура, розробка. Управління ризиками інформаційної безпеки: методологія оцінки ризиків, якісні та кількісні методи. Методи обробки ризиків: прийняття, уникнення, передача, зниження.

Лабораторна (2 год.): Розробка моделі загроз для навчальної ІС; визначення політики контролю доступу за RBAC-моделлю; практичний розрахунок ризиків за методологією DREAD.

СРС (7 год.): Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах» (КУБГ, 2024) — розділ «Моделі безпеки»; підготовка реферату «Порівняльний аналіз моделей контролю доступу в сучасних ОС».

Тема 1.4 — Оцінювання захищеності та аудит ІБ (Лекція 4, 2 год.)

Поняття захищеності інформаційної системи. Критерії оцінювання захищеності: НД ТЗІ 2.5-004-99, Common Criteria (ISO/IEC 15408). Класи захищеності автоматизованих систем. Поняття та цілі аудиту інформаційної безпеки. Методи проведення аудиту: технічний аудит, організаційний аудит, тестування на проникнення (пентест). Інструментальні засоби аудиту безпеки.

Лабораторна (2 год.): Практичне застосування інструментів аудиту (Nmap, OpenVAS, OWASP ZAP) для аналізу захищеності навчальної системи; оформлення звіту аудиту за стандартними вимогами.

СРС (7 год.): Опрацювання: Терейковський І. А., Гнатюк С. О. «Захист інформації в комп'ютерних системах» (КПІ, 2022) — розділ «Оцінювання захищеності»; підготовка порівняльної таблиці «Критерії захищеності ІС за НД ТЗІ та Common Criteria».

МОДУЛЬ 2

Криптографічні методи захисту інформації

Тема 2.1

Основи криптографії. Симетричні криптосистеми. Алгоритми AES, ДСТУ ГОСТ 28147-2009 (Калина).

Тема 2.2

Асиметричні криптосистеми. Алгоритми RSA, ECC. Криптографія на еліптичних кривих.

Тема 2.3

Хеш-функції та цифровий підпис. Стандарти ЕЦП. Інфраструктура відкритих ключів (PKI).

Тема 2.4

Криптографічні протоколи: TLS/SSL, IPsec, SSH. Стеганографія та приховування даних.

МОДУЛЬ 2 · ТЕМА 2.1

Основи криптографії. Симетричні криптосистеми.

Лекційний матеріал (2 год.)

Основні поняття криптології: криптографія, криптоаналіз, шифр, ключ. Класифікація криптосистем: симетричні, асиметричні, гібридні. Класичні шифри: підстановки, перестановки, Цезаря, Віженера. Блокові та потокові шифри. Стандарт шифрування AES: структура, раунди, режими роботи. Національний стандарт України: ДСТУ ГОСТ 28147-2009 та алгоритм «Калина» (ДСТУ 7624:2014). Управління ключами: генерація, розподіл, зберігання.

Ключові питання

- Принципи Керкгоффса та Шеннона в криптографії
- Порівняння блокових і потокових шифрів
- Режими роботи блокових шифрів (ECB, CBC, CTR, GCM)
- Особливості національного стандарту шифрування «Калина»
- Проблема розподілу ключів у симетричній криптографії

Лабораторне заняття (2 год.)

Завдання 1. Програмна реалізація алгоритму шифрування AES у різних режимах роботи (ECB, CBC); порівняння результатів шифрування однакових блоків даних.

Завдання 2. Криптоаналіз класичних шифрів: дешифрування тексту, зашифрованого шифром підстановки, методом частотного аналізу.

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

Самостійна робота (7 год.)

- Опрацювання: Самойлов І. В., Матійко А. А., Сторчак А. С. «Криптографія» (КПІ, 2023) — розділи «Симетричні криптосистеми», «AES»
- Підготовка реферату: «Алгоритм Калина (ДСТУ 7624:2014): структура та переваги перед попередниками»
- Складання порівняльної таблиці симетричних алгоритмів шифрування за ключовими характеристиками

Очікуваний результат: студент вміє описувати принципи симетричної криптографії, застосовувати алгоритм AES та розуміти особливості національного стандарту шифрування.

МОДУЛЬ 2 · ТЕМА 2.2

Асиметричні криптосистеми

Концепція

Відкритий і закритий ключ. Проблема дискретного логарифму та факторизації.

Diffie–Hellman

Протокол обміну ключами. Захищений канал без попереднього обміну секретом.

Постквантова

Загрози квантових комп'ютерів. Постквантові алгоритми NIST PQC.

RSA

Алгоритм Рівеста–Шаміра–Адлемана. Генерація ключів, шифрування, дешифрування.

ECC

Криптографія на еліптичних кривих. ECDSA, ECDH. Переваги перед RSA.

Лекційний матеріал (2 год.)

Принципи асиметричної криптографії: відкриті та закриті ключі, однобічні функції. Алгоритм RSA: математичні основи, генерація ключів, операції шифрування/дешифрування, вразливості. Протокол Діффі-Гелмана. Криптографія на еліптичних кривих (ECC): математичні основи, переваги. ECDSA та ECDH. Постквантова криптографія: загрози з боку квантових комп'ютерів та перспективні алгоритми.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Програмна реалізація алгоритму RSA: генерація ключів, шифрування та дешифрування тестового повідомлення; аналіз вразливостей при малих параметрах; практичне порівняння RSA та ECC за розміром ключів і швидкодією.

СРС: Опрацювання: Самойлов І. В., Матійко А. А., Сторчак А. С. «Криптографія» (КПІ, 2023) — розділ «Асиметричні системи»; підготовка аналітичної записки «Постквантова криптографія: стан стандартизації та перспективи впровадження».

МОДУЛЬ 2 · ТЕМИ 2.3–2.4

Цифровий підпис, PKI та криптографічні протоколи

Тема 2.3 — Хеш-функції та цифровий підпис (Лекція 7, 2 год.)

Криптографічні хеш-функції: властивості (однобічність, стійкість до колізій), SHA-2, SHA-3, ГОСТ 34.11. Національний стандарт хешування «Купина» (ДСТУ 7564:2014). Електронний цифровий підпис (ЕЦП): принципи, схеми DSA, ECDSA, ДСТУ 4145-2002. Інфраструктура відкритих ключів (PKI): сертифікати X.509, центри сертифікації, CRL, OCSP. Акредитовані центри сертифікації ключів в Україні.

Лабораторна (2 год.): Реалізація функцій хешування (SHA-256, SHA-3) та порівняння їх характеристик; формування та перевірка електронного цифрового підпису засобами Python/OpenSSL; аналіз структури X.509 сертифіката реального ЦСК.

СРС (7 год.): Опрацювання: Вишняков В. М. «Захист інформації в комп'ютерних системах» (КНУБА, 2022) — розділ «Криптографічний захист»; підготовка реферату «Система PKI в Україні: ЦСК, кваліфікований ЕЦП та електронна ідентифікація».

Тема 2.4 — Криптографічні протоколи та стеганографія (Лекція 8, 2 год.)

Криптографічні протоколи захисту каналів зв'язку: TLS/SSL (версії, рукостискання, шифрувальні набори), SSH (аутентифікація, тунелювання), IPsec (режими AH і ESP). HTTPS та захист вебзастосунків. Протоколи автентифікації: Kerberos, RADIUS, OAuth 2.0 та OpenID Connect. Стеганографія: принципи приховування даних у зображеннях, аудіо, текстах. Методи стегоаналізу.

Лабораторна (2 год.): Налаштування захищеного TLS-з'єднання з аналізом рукостискання засобами Wireshark; практичне використання SSH для захищеного з'єднання та тунелювання; базова реалізація LSB-стеганографії у зображеннях.

СРС (7 год.): Підготовка аналітичної записки «Безпека TLS 1.3: нові можливості та відмінності від попередніх версій»; аналіз вразливостей популярних криптографічних протоколів за звітами CERT-UA (2023–2024).

МОДУЛЬ 3

Захист комп'ютерних мереж та програмного забезпечення

Тема 3.1

Архітектура мережевої безпеки. Міжмережеві екрани (Firewall). Системи виявлення та запобігання вторгненням (IDS/IPS).

Тема 3.2

VPN-технології. Безпека бездротових мереж (Wi-Fi). Захист хмарних середовищ та SDN-мереж.

Тема 3.3

Безпека програмного забезпечення. Вразливості вебзастосунків (OWASP Top 10). Безпечна розробка ПЗ (SDLC).

Тема 3.4

Шкідливе програмне забезпечення (malware): класифікація, механізми дії, методи виявлення та протидії.

МОДУЛЬ 3 · ТЕМА 3.1

Архітектура мережевої безпеки. Міжмережеві екрани. IDS/IPS.

Лекційний матеріал (2 год.)

Модель OSI та загрози на різних рівнях мережевого стеку. Архітектура системи захисту мережі: демілітаризована зона (DMZ), сегментація мережі. Міжмережеві екрани (Firewall): покоління, типи (пакетна фільтрація, stateful inspection, NGFW), правила фільтрації. Системи виявлення вторгнень (IDS): сигнатурний та аномальний методи. Системи запобігання вторгненням (IPS). Захист від DDoS-атак. Honeypot та honeynets.

Ключові питання

- Загрози на рівнях мережевої моделі OSI та TCP/IP
- Покоління міжмережевих екранів та принципи їх роботи
- Відмінності між IDS та IPS, переваги та недоліки підходів
- Архітектура DMZ та її роль у захисті периметру мережі
- Механізми виявлення та пом'якшення DDoS-атак

Лабораторне заняття (2 год.)

Завдання 1. Налаштування правил міжмережевого екрана (iptables/nftables або pfSense) для захисту модельної мережі; аналіз журналів подій брандмауера.

Завдання 2. Практична робота з системою виявлення вторгнень Snort: написання власних правил для виявлення типових мережевих атак, аналіз зафіксованих подій.

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» (КУБГ, 2024) — розділ «Мережева безпека»
- Підготовка реферату: «Міжмережеві екрани нового покоління (NGFW): архітектура та можливості»
- Аналіз мережевого трафіку за допомогою Wireshark: виявлення аномалій та ознак атак

Очікуваний результат: студент вміє описувати архітектуру мережевої безпеки, налаштовувати базові правила Firewall та аналізувати роботу систем IDS/IPS.

МОДУЛЬ 3 · ТЕМА 3.2

VPN, бездротові мережі та хмарна безпека

Лекційний матеріал (2 год.)

VPN-технології: принципи побудови, типи (site-to-site, remote access), протоколи (IPsec, OpenVPN, WireGuard). Безпека бездротових мереж: протоколи WEP, WPA, WPA2, WPA3 — порівняння та вразливості. Атаки на Wi-Fi: Evil Twin, KRACK, деавтентифікація. Безпека хмарних обчислень: моделі хмар (IaaS, PaaS, SaaS), розподіл відповідальності за безпеку, загрози хмарних середовищ. Захист у SDN-мережах та NFV. Концепція Zero Trust Architecture.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Розгортання та налаштування VPN-сервера на базі WireGuard; аналіз вразливостей Wi-Fi-протоколів (на навчальному стенді); огляд механізмів безпеки хмарних платформ AWS/Azure/GCP та порівняльний аналіз їх налаштувань.

СРС: Опрацювання: Терейковський І. А., Гнатюк С. О. «Захист інформації в комп'ютерних системах» (КПІ, 2022) — розділ «Захист мережі»; підготовка аналітичної записки «Zero Trust Architecture: принципи, реалізація, актуальність для корпоративних мереж»; складання порівняльної таблиці VPN-протоколів.

Очікуваний результат: студент вміє характеризувати технології VPN, оцінювати захищеність бездротових мереж та описувати особливості безпеки хмарних середовищ.

МОДУЛЬ 3 · ТЕМА 3.3

Безпека програмного забезпечення та вебзастосунків

Вразливості коду (OWASP Top 10)

SQL-ін'єкція, XSS, CSRF, XXE, IDOR, небезпечна десеріалізація. Практика виявлення та усунення.

Безпечна розробка ПЗ (S-SDLC)

Інтеграція безпеки на всіх етапах: вимоги, проектування, реалізація, тестування, розгортання.

Тестування безпеки (SAST/DAST)

Статичний та динамічний аналіз коду. Fuzzing. Пентест вебзастосунків. Інструменти: Burp Suite, SonarQube.

Лекційний матеріал (2 год.)

Типові вразливості програмного забезпечення: переповнення буфера, ін'єкції, неправильна обробка помилок. OWASP Top 10: класифікація критичних вразливостей вебзастосунків. Безпечний цикл розробки ПЗ (S-SDLC): моделювання загроз, огляд коду, тестування безпеки. Методи тестування: SAST (статичний аналіз), DAST (динамічний аналіз), ручне тестування на проникнення. Захист від ін'єкцій: параметризовані запити, ORM, WAF.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Виявлення та експлуатація вразливостей OWASP Top 10 на навчальній платформі DVWA (Damn Vulnerable Web Application); усунення знайдених вразливостей; статичний аналіз коду за допомогою SonarQube.

СРС: Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах» (КУБГ, 2024) — розділ «Безпека вебзастосунків»; підготовка реферату «OWASP Top 10 2023: нові загрози та методи протидії».

МОДУЛЬ 3 · ТЕМА 3.4

Шкідливе програмне забезпечення: класифікація та протидія

Лекційний матеріал (2 год.)

Класифікація шкідливого програмного забезпечення (malware): віруси, черв'яки, трояни, ransomware, spyware, rootkits, бекдори, APT-загрози. Механізми поширення та зараження: фішинг, drive-by download, supply chain attacks. Принципи роботи антивірусного ПЗ: сигнатурний, евристичний, поведінковий аналіз, пісочниця (sandbox). Сучасні APT-загрози проти України: аналіз звітів CERT-UA та SBU. Відповідь на інциденти (Incident Response): PICERL-методологія.

Ключові питання

- Різниця між вірусами, черв'яками та троянами
- Механізми дії ransomware та методи захисту
- APT-угруповання та їх методи (TTP за MITRE ATT&CK)
- Методи виявлення malware: переваги та обмеження
- PICERL: підготовка, виявлення, стримування, знищення, відновлення

Лабораторне заняття (2 год.)

Завдання 1. Аналіз поведінки зразків malware у ізольованому середовищі (пісочниця Any.run/Cuckoo Sandbox): визначення типу, механізмів роботи та індикаторів компрометації (IoC).

Завдання 2. Практична робота з фреймворком MITRE ATT&CK: картографування тактик та технік реальної APT-групи за відкритими звітами CERT-UA.

Завдання 3. Розробка плану реагування на інцидент (Incident Response Plan) для типового кіберінциденту на підприємстві.

Самостійна робота (7 год.)

- Опрацювання: Вишняков В. М. «Захист інформації в комп'ютерних системах» (КНУБА, 2022) — розділ «Шкідливе ПЗ»
- Підготовка аналітичної записки «Кібератаки проти України 2022–2024: аналіз тактик та технік за звітами CERT-UA»
- Складання таблиці «Сучасні типи malware: механізми дії та засоби протидії»

Очікуваний результат: студент вміє класифікувати шкідливе ПЗ, аналізувати його поведінку, застосовувати MITRE ATT&CK та розробляти плани реагування на інциденти.

МОДУЛЬ 4

Комплексні системи захисту та практична безпека

Тема 4.1

Управління ідентифікацією та доступом (IAM). Автентифікація: паролі, багатофакторна автентифікація (MFA), біометрія.

Тема 4.2

Захист баз даних та резервне копіювання. Шифрування даних у спокої та в русі. СУБД і безпека.

Тема 4.3

Соціальна інженерія та людський фактор. Фішинг, вішинг, претекстинг. Навчання та культура безпеки.

Тема 4.4

Комплексна система захисту інформації (КСЗІ). Проектування, впровадження та атестація КСЗІ за вимогами НД ТЗІ.

МОДУЛЬ 4 · ТЕМА 4.1

Управління ідентифікацією та доступом (IAM)

Лекційний матеріал (2 год.)

Поняття ідентифікації, автентифікації та авторизації (IAA). Фактори автентифікації: знання, володіння, притаманність. Парольна безпека: вимоги до паролів, атаки на паролі (brute force, dictionary, rainbow tables), захист хешуванням з сіллю (bcrypt, Argon2). Багатофакторна автентифікація (MFA): TOTP, HOTP, FIDO2/WebAuthn. Біометрична автентифікація: методи, переваги та ризики. Системи Single Sign-On (SSO): SAML, OAuth 2.0, OpenID Connect. Управління привілейованим доступом (PAM).

Ключові питання

- Відмінності між ідентифікацією, автентифікацією та авторизацією
- Атаки на паролі та сучасні методи захисту
- Принципи роботи TOTP та FIDO2/WebAuthn
- Ризики та переваги біометричної автентифікації
- Архітектура SSO та протоколи OAuth 2.0 / SAML

Лабораторне заняття (2 год.)

Завдання 1. Реалізація системи автентифікації з MFA (TOTP) на основі Google Authenticator або Authy: налаштування, тестування, аналіз стійкості.

Завдання 2. Практична атака на слабкі паролі: злам хешів MD5 та SHA-1 методом rainbow tables; порівняння з bcrypt та Argon2 — оцінка часу зламу.

Завдання 3. Налаштування рольової моделі доступу (RBAC) для модельного застосунку; аналіз принципу найменших привілеїв.

Самостійна робота (7 год.)

- Опрацювання: Терейковський І. А., Корченко А. О. «Інтелектуалізовані методи захисту інформації» (КПІ, 2022) — розділ «Автентифікація»
- Підготовка реферату «FIDO2/WebAuthn: безпарольна автентифікація як майбутнє захисту облікових записів»
- Аналіз звітів про витоки даних (Have I Been Pwned, HackRead): типові причини та наслідки

Очікуваний результат: студент вміє описувати методи автентифікації, налаштовувати MFA, аналізувати стійкість парольного захисту та обирати відповідні засоби IAM.

МОДУЛЬ 4 · ТЕМА 4.2

Захист баз даних та резервне копіювання

Лекційний матеріал (2 год.)

Загрози безпеці баз даних: SQL-ін'єкції, несанкціонований доступ, витоки даних. Механізми захисту СУБД: контроль доступу, шифрування стовпців і таблиць, аудит операцій, маскування даних. Шифрування даних у спокої (at rest): TDE (Transparent Data Encryption) та шифрування на рівні файлів. Шифрування даних у русі (in transit): TLS/SSL для з'єднань з СУБД. Стратегії резервного копіювання: 3-2-1 правило, типи резервних копій. Захист резервних копій від шифрувальників (ransomware). GDPR та Закон про захист персональних даних: вимоги до обробки та захисту ПДн.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Налаштування захищеного з'єднання з СУБД PostgreSQL через TLS; реалізація маскування та шифрування чутливих полів бази даних; налаштування аудиту операцій та аналіз журналів; розробка та тестування стратегії резервного копіювання.

СРС: Опрацювання: Костюк Ю. В., Складанний П. М. «Захист інформації в комп'ютерних системах та мережах» (КУБГ, 2024) — розділ «Захист даних»; підготовка аналітичної записки «Захист персональних даних в Україні: вимоги законодавства та практика впровадження»; складання хронологічної таблиці «Найбільші витоки баз даних в Україні 2022–2024 рр.».

Очікуваний результат: студент вміє налаштовувати базові засоби захисту СУБД, реалізовувати стратегії резервного копіювання та описувати вимоги законодавства щодо захисту персональних даних.

МОДУЛЬ 4 · ТЕМА 4.3

Соціальна інженерія та людський фактор у безпеці

Лекційний матеріал (2 год.)

Психологічні основи соціальної інженерії: принципи Чалдіні (авторитет, терміновість, взаємність, соціальний доказ). Методи атак: фішинг, спір-фішинг, вішинг, смішинг, претекстинг, фізичне проникнення. OSINT-інструменти. Людський фактор як найслабша ланка в системі безпеки. Програми підвищення обізнаності персоналу (Security Awareness Training). Симуляції фішингових атак. Технічні засоби захисту від соціальної інженерії: SPF, DKIM, DMARC, антифішингові системи.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Практична OSINT-розвідка (на навчальному стенді/легальних ресурсах) із побудовою профілю об'єкта; симуляція фішингової кампанії засобами GoPhish; налаштування DMARC для захисту від підробки відправника.

СРС: Опрацювання: Вишняков В. М. «Захист інформації в комп'ютерних системах» (КНУБА, 2022) — розділ «Соціальна інженерія»; підготовка аналітичної записки «Фішингові атаки в Україні 2023–2024 рр. за звітами CERT-UA: методи та тенденції»; розробка модуля навчання персоналу з кібергігієни для умовного підприємства.

МОДУЛЬ 4 · ТЕМА 4.4

Комплексна система захисту інформації (КСЗІ)

Лекційний матеріал (2 год.)

Поняття комплексної системи захисту інформації (КСЗІ). Вимоги нормативних документів НД ТЗІ до побудови КСЗІ. Етапи створення КСЗІ: обстеження об'єкта, розробка технічного завдання, проектування, впровадження, атестація. Технічний захист інформації (ТЗІ): організаційні, технічні та криптографічні заходи. Безпека критичної інфраструктури в Україні. Система управління інформаційною безпекою (ISMS) за ISO/IEC 27001: цикл PDCA. Кіберстійкість (Cyber Resilience) як стратегічний підхід.

Ключові питання

- Вимоги НД ТЗІ до КСЗІ: класи захисту та необхідні засоби
- Процес атестації КСЗІ в Україні
- Захист об'єктів критичної інфраструктури: вимоги та стандарти
- ISMS за ISO/IEC 27001: структура та процеси
- Кіберстійкість: від захисту до відновлення після інцидентів

Лабораторне заняття (2 год.)

Завдання 1. Розробка концепції КСЗІ для модельної автоматизованої системи: визначення класу ІС, переліку загроз, необхідних засобів захисту відповідно до НД ТЗІ.

Завдання 2. Підготовка та захист міні-проекту «Аудит інформаційної безпеки умовного підприємства за ISO/IEC 27001»: виявлення невідповідностей, рекомендації щодо впровадження засобів захисту.

Завдання 3. Фінальне тестування за курсом (підсумковий тест — 20 питань з усіх модулів).

Самостійна робота (7 год.)

- Опрацювання: Терейковський І. А., Гнатюк С. О. «Захист інформації в комп'ютерних системах» (КПІ, 2022) — розділ «КСЗІ»
- Підготовка аналітичної записки «Кіберстійкість критичної інфраструктури України: стан та перспективи»
- Аналіз вимог Закону «Про основні засади забезпечення кібербезпеки України» та Стратегії кібербезпеки

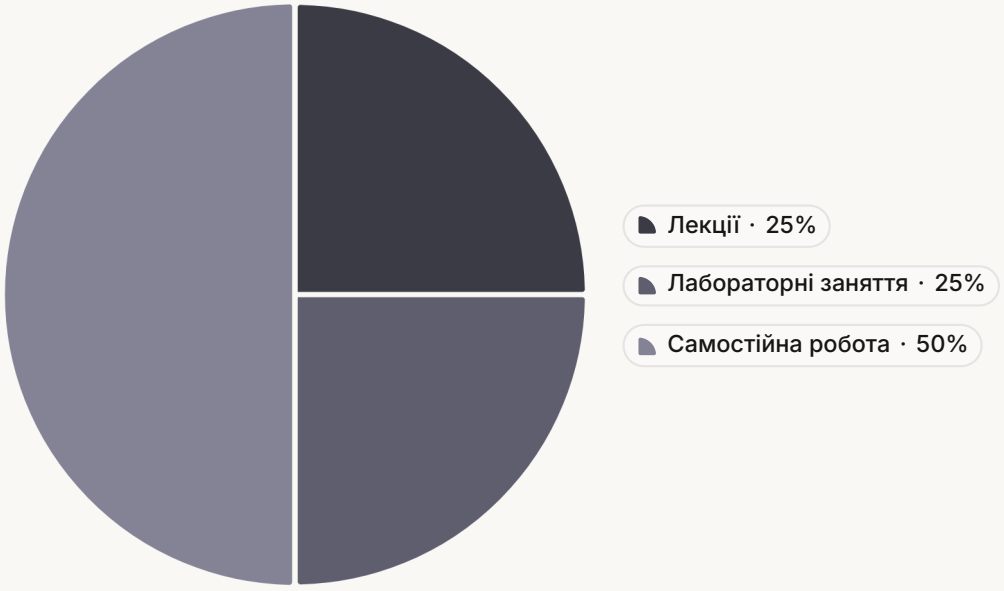
Очікуваний результат: студент вміє проектувати концепцію КСЗІ, застосовувати вимоги НД ТЗІ та стандарту ISO/IEC 27001, обґрунтовувати вибір засобів захисту інформації.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Основи ІБ, загрози та вразливості	2	2	7
	Тема 1.2 — Нормативно-правова база	2	2	7
	Тема 1.3 — Моделі безпеки та управління ризиками	2	2	7
	Тема 1.4 — Оцінювання захищеності та аудит ІБ	2	2	7
Модуль 2	Тема 2.1 — Симетричні криптосистеми	2	2	7
	Тема 2.2 — Асиметричні криптосистеми	2	2	7
	Тема 2.3 — Хеш-функції, ЕЦП та PKI	2	2	7
	Тема 2.4 — Криптографічні протоколи та стеганографія	2	2	7
Модуль 3	Тема 3.1 — Мережева безпека: Firewall, IDS/IPS	2	2	7
	Тема 3.2 — VPN, Wi-Fi, хмарна безпека	2	2	7
	Тема 3.3 — Безпека ПЗ та вебзастосунків	2	2	7
	Тема 3.4 — Шкідливе ПЗ та реагування на інциденти	2	2	7
Модуль 4	Тема 4.1 — Управління ідентифікацією та доступом	2	2	7
	Тема 4.2 — Захист баз даних та резервне копіювання	2	2	7
	Тема 4.3 — Соціальна інженерія та людський фактор	2	2	7
	Тема 4.4 — КСЗІ та комплексний захист	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 теорією та практикою.

Лекції — 30 год. (25%)

Системне подання ключового теоретичного матеріалу з використанням наочних схем, діаграм та прикладів реальних кіберінцидентів і атак.

Лабораторні — 30 год. (25%)

Практичне відпрацювання навичок у захищеному навчальному середовищі: налаштування засобів захисту, аналіз атак, реалізація криптографічних алгоритмів. Рівна частка з лекціями підкреслює практичну спрямованість курсу.

Самостійна робота — 60 год. (50%)

Поглиблене вивчення, підготовка звітів, робота з нормативною документацією та науковою літературою. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками та посібниками з захисту інформації (Терейковський, Гнатюк, Вишняков, Костюк, Самойлов та ін.), нормативними документами НД ТЗІ, стандартами ISO/IEC 27000, науковими статтями у фахових виданнях. Студент конспектує ключові положення та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (аналіз кіберінцидентів, порівняння засобів захисту, оцінка ризиків); творчих завдань — реферати, аналітичні записки, міні-дослідження з актуальних питань кібербезпеки та захисту інформації.

Робота з інформаційними ресурсами

Опрацювання офіційних ресурсів: CERT-UA (**cert.gov.ua**), Держспецзв'язку (**cip.gov.ua**), ДССЗІ (**dsszzi.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**), NIST Cybersecurity Framework. Аналіз звітів кіберінцидентів, пошук актуальної інформації для навчальних завдань.

Підготовка до занять

Підготовка до лабораторних занять (опрацювання методичних матеріалів, розуміння інструментарію); підготовка до тестувань (ключові терміни та концепції); підготовка до контрольних робіт за кожним модулем (систематизація знань, типові питання).

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 захисту лабораторної роботи.	Модульна контрольна робота або комплексне лабораторне завдання, яке охоплює теми змістовного модуля (теоретичні питання, практичні завдання з налаштування засобів захисту, аналіз ситуацій). Оцінюються повнота відповіді, правильність виконання та обґрунтованість висновків. Проводиться після завершення кожного змістовного модуля.	Іспит відповідно до навчального плану. Форма проведення — тестування та практичне завдання. 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 інформації в комп'ютерних системах» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок, необхідних для майбутньої інженерної діяльності у сфері комп'ютерних технологій та кібербезпеки.

Лекції

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

Робота з нормативними документами

Опрацювання нормативних документів НД ТЗІ, стандартів ISO/IEC 27000, законодавчих актів у сфері кібербезпеки; формування навичок застосування вимог у практичних задачах.

Кейс-стаді

Аналіз реальних кіберінцидентів та кейсів із практики CERT-UA; студенти виявляють вектор атаки, визначають наслідки та пропонують заходи захисту.

Лабораторний практикум

Практична реалізація засобів захисту, криптографічних алгоритмів та інструментів аналізу у контрольованому навчальному середовищі; розвиток практичних компетентностей.

Самостійне дослідження

Підготовка аналітичних записок, рефератів і міні-проектів з актуальних питань кібербезпеки; розвиток навичок самостійного пошуку та критичного аналізу інформації.

Тестування на проникнення

Виконання контрольованих пентест-вправ на навчальних вразливих платформах (DVWA, HackTheBox EDU); безпечне засвоєння методів атаки для розуміння захисту.

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

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

1. Терейковський І. А., Гнатюк С. О.
Захист інформації в комп'ютерних системах : навч. посіб. для здобувачів ступеня бакалавра спеціальності 123 Комп'ютерна інженерія. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 127 с.

2. Вишняков В. М.
Захист інформації в комп'ютерних системах : навч. посіб. — Київ : КНУБА, 2022. — 119 с.

3. Самойлов І. В., Матійко А. А., Сторчак А. С.
Криптографія : навч. посіб. для здобувачів першого (бакалаврського) рівня вищої освіти. — Київ : КПІ ім. Ігоря Сікорського, 2023.

4. Костюк Ю. В., Складанний П. М.
Захист інформації в комп'ютерних системах та мережах. Частина І : підручник. — Київ : Київський столичний університет імені Бориса Грінченка, 2024. — 401 с.

5. Терейковський І. А., Корченко А. О.
Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації : навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 176 с.

6. Гнатюк С. О. та ін.
Захист інформації в комп'ютерних системах і кібербезпека (Частина 1) : навч. посіб. — Київ : НУБіП України, 2023.

7. Євсеєв С. П., Остапов С. Е., Король О. Г.
Кібербезпека: сучасні технології захисту : навч. посіб. для студентів вищих навчальних закладів. — Львів : Новий Світ-2000, 2022.

8. Грайворонський М. В., Новіков О. М.
Безпека інформаційно-комунікаційних систем : підручник. — 2-ге вид., перероб. та доп. — Київ : BHV, 2022. — 608 с.

Додаткова література та наукові ресурси

9. Лісовська Ю. П.

Кібербезпека: ризики та заходи : навч. посіб. — Львів, 2023. *Рекомендується для тем 1.1–1.4 (основи ІБ та управління ризиками).*

10. Звіти CERT-UA

Щорічні та тематичні звіти про кіберзагрози та інциденти в Україні. — **cert.gov.ua**, 2022–2024. *Рекомендується для тем 3.4 та 4.3–4.4.*

11. Єршова О. О., Гончаренко І. М.

Сучасні підходи до забезпечення кібербезпеки підприємств в умовах воєнного стану. Журнал стратегічних економічних досліджень. — 2023. — № 3. *Рекомендується для тем 4.3–4.4.*

12. NIST Cybersecurity Framework 2.0

National Institute of Standards and Technology. Cybersecurity Framework 2.0. — 2024. **nist.gov/cyberframework**. *Рекомендується для модулів 1 та 4.*

Нормативно-правова база

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

  Основний нормативний акт у сфері захисту інформації. **zakon.rada.gov.ua**

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

  Засади кібербезпеки, об'єкти критичної інфраструктури, повноваження органів. **zakon.rada.gov.ua**

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

  Вимоги до обробки та захисту персональних даних. **zakon.rada.gov.ua**

- НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в КС від НСД»

  Основні терміни та визначення у сфері технічного захисту інформації від несанкціонованого доступу.

- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД»

  Критерії та класи захищеності автоматизованих систем від несанкціонованого доступу.

Офіційні ресурси та фахові видання

CERT-UA

cert.gov.ua — Урядова команда реагування на надзвичайні події у сфері кібербезпеки України: звіти про інциденти, попередження, аналітика.

Держспецзв'язку (ДССЗІ)

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

Верховна Рада України

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

Національна бібліотека України ім. В. І. Вернадського

nbuv.gov.ua — Електронні ресурси, наукові статті, монографії з інформаційної безпеки та кібербезпеки.

Журнал «Захист інформації»

Фахове наукове видання Національного авіаційного університету з питань інформаційної безпеки та захисту даних.

OWASP Foundation

owasp.org — Відкрита база знань з безпеки вебзастосунків, методології, інструменти та стандарти.

MITRE ATT&CK

attack.mitre.org — Фреймворк тактик та технік кіберзловмисників для аналізу загроз та побудови захисту.

Міністерство освіти і науки України

mon.gov.ua — Освітні стандарти, навчальні програми, методичні матеріали для спеціальності 123.

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

Чому «Захист інформації» для інженерів?

Дисципліна «Захист інформації в комп'ютерних системах» є невід'ємною складовою підготовки бакалаврів зі спеціальністю 123 «Комп'ютерна інженерія». Будь-яка комп'ютерна система, розроблена або налаштована інженером, є потенційним об'єктом кіберзагроз — без знань у сфері захисту інформації неможливо проектувати надійні системи.

Сучасний фахівець у сфері комп'ютерної інженерії проектує апаратно-програмні комплекси, вбудовані системи та мережеву інфраструктуру, де безпека є не додатковою опцією, а обов'язковою вимогою замовника та регулятора.

Практичне значення для майбутньої кар'єри

- Проектування безпечних комп'ютерних систем та мереж з урахуванням вимог НД ТЗІ
- Розуміння криптографічних протоколів для розробки захищених комунікаційних систем
- Навички аналізу вразливостей для відповідального тестування власних розробок
- Знання нормативної бази для роботи на об'єктах критичної інфраструктури України
- Конкурентна перевага на ринку праці: попит на фахівців з кібербезпеки зростає щорічно
- Основа для подальшого навчання за спеціальністю 125 «Кібербезпека та захист інформації»

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові аспекти захисту інформації — від теоретичних основ та криптографії до мережевої безпеки та проектування комплексних систем захисту — і формує у студентів цілісне розуміння сучасного ландшафту кіберзагроз та засобів протидії їм.

Бажаємо успіхів у вивченні захисту інформації!

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

16

Тем

У 4 змістовних модулях

8+

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Безпека — це не продукт, а процес.» — Брюс Шнайер

Спеціальність 123 · Комп'ютерна інженерія · Бакалавр · 4 кредити ЄКТС