Силабус 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

Змістовних модулі 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 курсу

Мета дисципліни

Дисципліна «Захист інформації в комп'ютерних системах» формує у студентів спеціальності «Комп'ютерна інженерія» системні знання та практичні навички у сфері забезпечення інформаційної безпеки комп'ютерних систем і мереж. Курс спрямований на вивчення сучасних методів і засобів захисту інформації, криптографічних алгоритмів, механізмів контролю доступу, а також правових та організаційних аспектів кібербезпеки. Особлива увага приділяється формуванню практичних компетентностей щодо виявлення загроз, проектування систем захисту та протидії кіберінцидентам у реальних умовах.

Форми навчання

- Лекції — 30 годин
- Лабораторні заняття — 30 годин
- Самостійна робота — 60 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання інформації у сфері інформаційної безпеки: виявлення вразливостей, порівняння методів захисту, формування обґрунтованих рішень щодо побудови систем безпеки. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки звітів з лабораторних робіт, аналітичних оглядів і технічних завдань.

Здатність до усної та письмової фахової комунікації: чітко формулювати технічні вимоги до систем захисту, аргументовано обґрунтовувати вибір засобів безпеки, оформлювати технічну документацію. Відповідальність, ініціативність і готовність працювати в команді під час виконання комплексних лабораторних і проєктних завдань.

- Аналізувати технічну та нормативну документацію в галузі ІБ
- Систематизувати та узагальнювати результати досліджень
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися з викладачами та одногрупниками
- Брати участь у командній роботі над проєктами безпеки

Фахові компетентності

Розуміння сутності загроз інформаційній безпеці, класифікації атак і вразливостей комп'ютерних систем. Знання основних криптографічних алгоритмів (симетричних, асиметричних, гешування), протоколів захисту мережевих комунікацій, а також вітчизняних і міжнародних стандартів у галузі кібербезпеки.

Здатність застосовувати сучасні методи і засоби захисту інформації для проєктування захищених комп'ютерних систем, реалізації політики безпеки, виявлення та нейтралізації кіберзагроз відповідно до вимог чинного законодавства України.

- Класифікувати загрози та вразливості комп'ютерних систем
- Застосовувати криптографічні методи захисту даних
- Налаштовувати засоби мережевої безпеки (firewall, VPN, IDS)
- Розробляти політику та моделі управління доступом
- Виявляти та реагувати на кіберінциденти

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять інформаційної безпеки: конфіденційність, цілісність, доступність, аутентифікація, авторизація, шифрування, електронний підпис, кіберзагроза, вразливість, інцидент безпеки. Характеризувати основні класи атак на комп'ютерні системи та методи протидії їм.

2

Аналіз та оцінювання

Аналізувати загрози та ризики для конкретної інформаційної системи, виявляти слабкі місця архітектури безпеки. Оцінювати ефективність різних криптографічних алгоритмів і протоколів захисту, порівнювати засоби і методи забезпечення інформаційної безпеки.

3

Застосування знань

Застосовувати методи та засоби захисту інформації для вирішення практичних задач: налаштування систем аутентифікації, шифрування каналів зв'язку, побудови демілітаризованих зон, реалізації політики безпеки відповідно до стандартів ISO/IEC 27001 та вітчизняних НД ТЗІ.

4

Комунікація та рефлексія

Аргументовано обстоювати прийняті рішення щодо вибору методів і засобів захисту інформації. Розуміти правові та етичні аспекти діяльності у сфері кібербезпеки, формувати відповідальне ставлення до захисту персональних даних та критичної інфраструктури.

Модуль 1. Основи інформаційної безпеки та загрози комп'ютерним системам

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Вступ до захисту інформації. Основні поняття та визначення. Тріада CIA (конфіденційність, цілісність, доступність). Класифікація інформації за ступенем секретності. Нормативно-правова база України у сфері захисту інформації: Закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про кібербезпеку».

Тема 1.2

Загрози та вразливості комп'ютерних систем. Класифікація загроз: випадкові та навмисні, внутрішні та зовнішні. Типи зловмисників та мотиви атак. Вразливості програмного та апаратного забезпечення. Поняття моделі загроз. Системи виявлення та запобігання вторгненням (IDS/IPS). OWASP Top 10.

Тема 1.3

Класифікація атак на комп'ютерні системи. Мережеві атаки: DoS/DDoS, MITM, спуфінг, сніфінг. Атаки на рівні застосунків: SQL-ін'єкція, XSS, CSRF. Соціальна інженерія та фішинг. Шкідливе програмне забезпечення: віруси, трояни, програми-вимагачі, шпигунське ПЗ. APT-загрози.

Тема 1.4

Стандарти та нормативна база захисту інформації. Міжнародні стандарти: ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework. Вітчизняні нормативні документи технічного захисту інформації (НД ТЗІ). Державна служба спеціального зв'язку та захисту інформації України. Порядок атестації та сертифікації систем захисту.

Модуль 2. Криптографічні методи захисту інформації

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Основи криптографії. Симетричне шифрування: алгоритми DES, 3DES, AES, ДСТУ 7624 (Калина). Режими роботи блокових шифрів: ECB, CBC, CTR, GCM. Потокові шифри. Криптоаналіз та оцінка стійкості. Управління ключами в симетричних системах.

Тема 2.2

Асиметрична криптографія та інфраструктура відкритих ключів. Алгоритми RSA, DSA, ECDSA. Алгоритм Діффі-Хеллмана. Вітчизняний стандарт ДСТУ 4145 (на еліптичних кривих). Цифровий підпис і його правовий статус в Україні. Інфраструктура відкритих ключів (PKI), сертифікати X.509, центри сертифікації.

Тема 2.3

Геш-функції та автентифікаційні коди. Геш-функції: MD5, SHA-1, SHA-2, SHA-3, ДСТУ 7564 (Купина). Коди автентифікації повідомлень (MAC, HMAC). Цифровий підпис на основі геш-функцій. Застосування геш-функцій у системах захисту: зберігання паролів, перевірка цілісності, блокчейн.

Модуль 3. Захист комп'ютерних мереж та систем

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Мережева безпека та засоби захисту периметру. Брандмауери (firewall): типи та принципи роботи. Демілітаризована зона (DMZ). Проксі-сервери та системи фільтрації контенту. Технології VPN: IPsec, OpenVPN, WireGuard. Протоколи захисту мережевих комунікацій: TLS/SSL, SSH, HTTPS. Безпека бездротових мереж (WPA3).

Тема 3.2

Аутентифікація та управління доступом. Методи аутентифікації: однофакторна, двофакторна (2FA), багатофакторна (MFA). Протоколи аутентифікації: Kerberos, RADIUS, OAuth 2.0, SAML. Моделі управління доступом: DAC, MAC, RBAC, ABAC. Засоби контролю доступу до ресурсів. Управління привілейованим доступом (PAM).

Тема 3.3

Безпека хмарних середовищ та IoT. Особливості захисту хмарних інфраструктур (IaaS, PaaS, SaaS). Модель спільної відповідальності. Безпека контейнерів і мікросервісів (Docker, Kubernetes). Загрози Інтернету речей (IoT) та методи захисту. Безпека операційних технологій (OT/SCADA). Захист критичної інфраструктури.

Модуль 4. Організаційно-правові засади та управління інформаційною безпекою

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Управління ризиками інформаційної безпеки. Поняття ризику та методологія управління ризиками (ISO 31000, NIST SP 800-30). Ідентифікація активів, загроз і вразливостей. Кількісна та якісна оцінка ризиків. Стратегії реагування: прийняття, уникнення, мінімізація, передача ризиків. Побудова системи управління інформаційною безпекою (СУІБ/ISMS).

Тема 4.2

Реагування на інциденти та відновлення після збоїв. Класифікація та пріоритизація інцидентів безпеки. Процес реагування на інциденти: виявлення, стримування, ліквідація, відновлення. Цифрова криміналістика (forensics) та збір доказів. Планування безперервності бізнесу (BCP) та відновлення після катастроф (DRP). SOC-центри кібербезпеки.

Тема 4.3

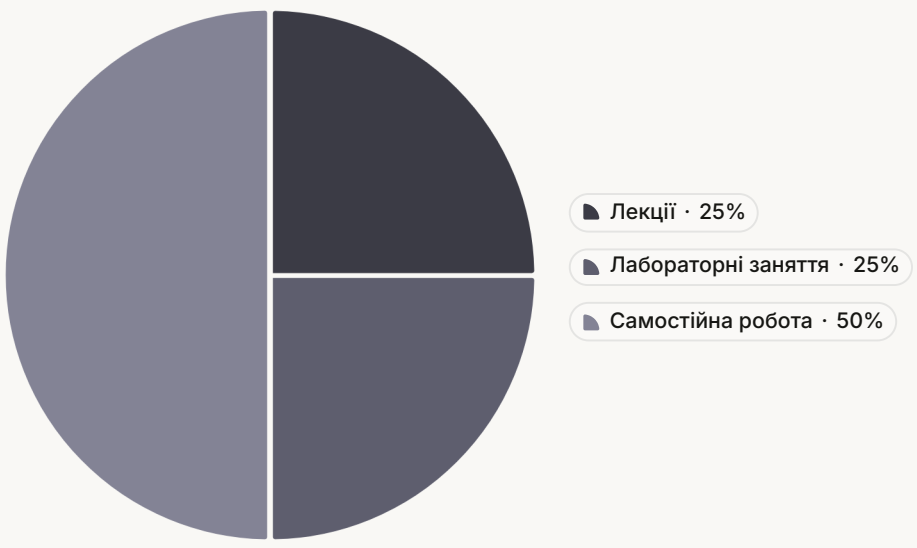
Правові та організаційні аспекти захисту інформації. Кіберзаконодавство України та відповідальність за кіберзлочини. Захист персональних даних: Закон України «Про захист персональних даних», GDPR. Організація служби інформаційної безпеки на підприємстві. Аудит і моніторинг безпеки. Пентестинг та оцінка захищеності систем.

Тема 4.4

Сучасні тенденції та виклики кібербезпеки. Кібербезпека в умовах збройного конфлікту: досвід України. Застосування штучного інтелекту у сфері кібербезпеки. Кіберрозвідка (Threat Intelligence). Zero Trust Architecture. Квантові загрози та постквантова криптографія. Державна кібербезпекова стратегія України.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Вступ до захисту інформації	2	2	4
	Тема 1.2 — Загрози та вразливості комп'ютерних систем	2	2	4
	Тема 1.3 — Класифікація атак на комп'ютерні системи	2	2	4
	Тема 1.4 — Стандарти та нормативна база захисту інформації	2	2	4
Модуль 2	Тема 2.1 — Основи криптографії (симетричне шифрування)	2	2	4
	Тема 2.2 — Асиметрична криптографія та PKI	2	2	4
	Тема 2.3 — Геш-функції та автентифікаційні коди	4	4	8
Модуль 3	Тема 3.1 — Мережева безпека та засоби захисту периметру	4	4	8
	Тема 3.2 — Аутентифікація та управління доступом	4	4	8
	Тема 3.3 — Безпека хмарних середовищ та IoT	2	2	4
Модуль 4	Тема 4.1 — Управління ризиками інформаційної безпеки	2	2	4
	Тема 4.2 — Реагування на інциденти та відновлення	2	2	4
	Тема 4.3 — Правові та організаційні аспекти захисту інформації	2	2	4
	Тема 4.4 — Сучасні тенденції та виклики кібербезпеки	2	2	4
Разом		**30**	**30**	**60**



Структура навчального часу

Загальний обсяг — **120 годин (4 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

- **Лекції (30 год. — 25%):** подача ключового теоретичного матеріалу
- **Лабораторні (30 год. — 25%):** відпрацювання практичних навичок захисту систем
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, підготовка завдань

Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються самостійно досліджувати методи та засоби захисту інформації.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками з захисту інформації, нормативними документами (НД ТЗІ), міжнародними стандартами (ISO/IEC 27001) та науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань з оцінки захищеності модельних систем, підготовка звітів з аналізу вразливостей, міні-досліджень сучасних кіберзагроз та засобів протидії. Написання аналітичних оглядів на актуальні теми кібербезпеки.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), CERT-UA (**cert.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**). Вивчення звітів щодо актуальних кіберзагроз, бюлетенів з вразливостей.

Підготовка до занять

Підготовка до лабораторних робіт шляхом вивчення відповідних інструментів та технологій захисту; повторення теоретичного матеріалу перед тестуванням; систематизація знань перед модульними контрольними роботами та підсумковим іспитом.

Методи викладання

Лекції

Системне подання теоретичного матеріалу з використанням схем, діаграм атак і засобів захисту, демонстрацій роботи інструментів; студенти ведуть конспекти та задають уточнювальні запитання.

Лабораторні роботи

Практичне налаштування засобів захисту, реалізація криптографічних алгоритмів, аналіз мережевого трафіку, конфігурація брандмауерів та VPN у захищеному лабораторному середовищі.

Кейс-стаді

Аналіз реальних кіберінцидентів і атак; студенти виявляють вектори атаки, пропонують заходи захисту та обґрунтовують вибір засобів безпеки на основі отриманих знань.

Робота з інструментами

Практичне застосування інструментів кібербезпеки: Wireshark, nmap, OpenSSL, Metasploit (у навчальному середовищі), HashCat; формування навичок роботи з реальними засобами захисту.

Самостійне дослідження

Підготовка аналітичних оглядів сучасних кіберзагроз, звітів з оцінки захищеності модельних систем; розвиток навичок самостійного пошуку та систематизації інформації в галузі ІБ.

Форми контролю знань

1

Поточний контроль

Завдання: тестові вправи та практичні завдання за темами змістовного модуля. Оцінюються регулярність виконання лабораторних робіт, якість звітів і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, захист лабораторних робіт, розв'язання ситуаційних завдань із забезпечення безпеки.

2

Проміжний контроль

Модульна контрольна робота — комплексне ситуаційне завдання або індивідуальна розрахунково-графічна робота, що охоплює теми змістовних модулів (теоретичні питання, практичне завдання з аналізу вразливостей або розробки моделі загроз). Оцінюються повнота відповіді, правильність виконання та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — тестування та письмові/практичні відповіді на питання з усіх розділів дисципліни. 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).

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

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах : навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022.
2. Вишняков В. М. Захист інформації в комп'ютерних системах : навч. посіб. — Київ : КНУБА, 2022. — 119 с.
3. Євсєєв С. П., Мілов О. В., Остапов С. Е., Сєвєрінов О. В. Кібербезпека: основи кодування та криптографії. — Харків : Новий Світ-2000, 2023. — 657 с.
4. Самойлов І. В., Матійко А. А., Сторчак А. С. Криптографія : навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2023.
5. Костюк Ю. В., Складанний П. М. Захист інформації в комп'ютерних системах та мережах. Ч. І : підручник. — Київ : Університет імені Бориса Грінченка, 2024. — 401 с.
6. Титова Н. М. Інформаційна безпека та кібербезпека держави : навч. посіб. — Київ : Ліра-К, 2023.
7. Гнатюк С. О., Сейлова Н. А. Кіберрозвідка та аналіз загроз : навч. посіб. — Київ : НАУ, 2023.
8. Корченко О. Г., Архипов О. Є., Казмірчук С. В. Системи виявлення вторгнень : монографія. — Київ : НАУ, 2022. — 264 с.
9. Дудикевич В. Б., Микитишин А. Г., Стоцька М. В. Комп'ютерна безпека та криптографія : навч. посіб. — Львів : Видавництво Львівської політехніки, 2023. — 312 с.
10. Хорошко В. О., Чередниченко В. С. Методи та засоби захисту інформації : підручник. — Київ : Юніверс, 2024. — 346 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA. — URL: **https://cert.gov.ua/**
3. Офіційний сайт Верховної Ради України (законодавство у сфері ІБ). — URL: **https://zakon.rada.gov.ua/**
4. Національний координаційний центр кібербезпеки. — URL: **https://ncsc.gov.ua/**
5. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
6. Репозитарій КПІ ім. Ігоря Сікорського (навч. матеріали з ІБ). — URL: **https://ela.kpi.ua/**
7. NIST Cybersecurity Framework (офіційний ресурс). — URL: **https://www.nist.gov/cyberframework**
8. Журнал «Захист інформації» (фахове видання). — URL: **https://захист-інформації.укр/**

Рекомендована література охоплює видання **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення.