Робоча програма дисципліни «Соціотехнічна безпека»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

3

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Соціотехнічна безпека

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: Організація захисту інформації в інформаційно-комунікаційних системах

Ступінь: Бакалавр

Обсяг: 90 годин / 3 кредити ЄКТС

Модулів: 3 змістовних блоки

Призначення дисципліни

Дисципліна «Соціотехнічна безпека» формує у студентів системне розуміння природи соціотехнічних загроз, методів соціальної інженерії та психологічних механізмів маніпуляції, що використовуються для несанкціонованого доступу до інформаційних систем. Курс охоплює методи виявлення, протидії та попередження соціотехнічних атак в інформаційно-комунікаційних системах.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» та забезпечує формування фахових компетентностей, передбачених освітньо-професійною програмою «Організація захисту інформації в інформаційно-комунікаційних системах».

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації про соціотехнічні загрози: виявлення векторів атак, порівняння методів захисту, формування обґрунтованих висновків щодо ризиків.

Комунікація

Здатність до усної та письмової комунікації з питань інформаційної безпеки: чітко описувати соціотехнічні загрози, аргументувати заходи захисту, складати аналітичні звіти та технічну документацію.

Самоорганізація

Уміння самостійно навчатися, планувати дослідницьку роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки кейсів, аналітичних записок і дослідницьких проектів.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групового аналізу реальних інцидентів, розробки сценаріїв атак і засобів протидії, захисту спільних проектів.

Студент повинен вміти: аналізувати соціотехнічні загрози та вразливості людського фактора; виявляти ознаки атак соціальної інженерії; планувати заходи організаційного захисту; коректно взаємодіяти в команді з питань безпеки; брати участь у розробці та впровадженні політик інформаційної безпеки.

Фахові компетентності

Знання соціотехнічних загроз

Розуміння природи та закономірностей соціотехнічних атак, їх класифікації, типових векторів і механізмів реалізації. Знання психологічних прийомів маніпуляції, методів фішингу, вішингу, смішингу, бейтингу та претекстингу в контексті захисту інформаційно-комунікаційних систем.

Аналіз ризиків та інцидентів

Здатність аналізувати реальні інциденти соціотехнічних атак, оцінювати рівень ризиків для організації, виявляти вразливості людського фактора та розробляти моделі загроз для інформаційно-комунікаційних систем.

Організаційний захист та протидія

Знання принципів організаційного захисту від соціотехнічних атак: розробка політик безпеки, проведення навчань та тренінгів для персоналу, впровадження процедур верифікації та аутентифікації в ІКС.

Нормативно-правова база

Орієнтування в нормативно-правовій базі у сфері кібербезпеки та захисту інформації в Україні; застосування стандартів і регуляторних вимог для забезпечення соціотехнічної безпеки організацій.

Результати навчання

01

Пояснення ключових понять

Пояснювати сутність ключових понять і явищ: соціотехнічна атака, соціальна інженерія, людський фактор, фішинг, вішинг, претекстинг, інсайдерська загроза, кібергігієна, модель загроз, політика безпеки.

02

Класифікація та аналіз атак

Класифікувати соціотехнічні атаки за типами, векторами та цілями; застосовувати методи аналізу реальних інцидентів, виявляти психологічні механізми маніпуляції та визначати вразливі ланки в системі захисту.

03

Розробка заходів захисту

Розробляти та обґрунтовувати комплекс організаційно-технічних заходів захисту від соціотехнічних атак; складати плани навчання персоналу, сценарії тестування обізнаності та регламенти реагування на інциденти.

04

Робота з нормативно-правовою базою

Орієнтуватися в нормативно-правовій та стандартизаційній базі з кібербезпеки; застосовувати вимоги законодавства України та міжнародних стандартів для організації захисту від соціотехнічних загроз.

МОДУЛЬ 1

Основи соціотехнічної безпеки та природа загроз

1

Тема 1.1

Соціотехнічна безпека як наукова дисципліна. Основні поняття, класифікація загроз та людський фактор в інформаційній безпеці

2

Тема 1.2

Психологічні основи соціальної інженерії. Механізми маніпуляції, когнітивні упередження та принципи впливу на поведінку користувачів

3

Тема 1.3

Класифікація та типологія соціотехнічних атак. Фішинг, вішинг, смішинг, бейтинг, претекстинг, інсайдерські загрози: методи та вектори

МОДУЛЬ 1 · ТЕМА 1.1

Соціотехнічна безпека як дисципліна. Людський фактор

Лекційний матеріал (2 год.)

Лекція 1: Предмет, об'єкт та завдання дисципліни «Соціотехнічна безпека». Поняття «соціотехнічна система» та «соціотехнічна загроза». Місце соціотехнічної безпеки в системі інформаційної та кібербезпеки. Людський фактор як найвразливіша ланка захисту інформаційно-комунікаційних систем.

Лекція 2: Статистика соціотехнічних інцидентів: світові та українські тенденції. Класифікація суб'єктів загроз: зовнішні зловмисники, інсайдери, необізнані користувачі. Мотиваційні чинники атак. Загальна модель соціотехнічної атаки.

Ключові питання лекцій

- Поняття «соціотехнічна безпека» та її складові
- Людський фактор як вектор атаки в ІКС
- Суб'єкти та мотиви соціотехнічних загроз
- Місце соціотехнічної безпеки в системі кібербезпеки
- Статистика та тенденції соціотехнічних інцидентів

Практичне заняття (1 год.)

Завдання 1. Складання класифікаційної таблиці «Соціотехнічні загрози: суб'єкти, мотиви, цілі». Аналіз реальних статистичних даних про кіберінциденти в Україні.

Завдання 2. Кейс: аналіз реального інциденту соціотехнічної атаки на українську організацію. Виявлення ролі людського фактора та вразливих ланок захисту.

Самостійна робота (5 год.)

- Опрацювання: Бурячок В. Л. та ін. «Інформаційна та кібербезпека: соціотехнічний аспект» — розділ «Соціотехнічна безпека: проблемні аспекти»
- Підготовка реферату: «Людський фактор як основна вразливість сучасних ІКС»
- Аналіз звіту CERT-UA про соціотехнічні інциденти за останній рік

Очікуваний результат: студент вміє визначати місце соціотехнічної безпеки в системі захисту ІКС, характеризувати роль людського фактора та класифікувати суб'єктів загроз.

МОДУЛЬ 1 · ТЕМА 1.2

Психологічні основи соціальної інженерії

1

Когнітивні упередження

Схильність до авторитету, терміновість, принцип взаємності, соціальний доказ — базові механізми маніпуляції.

2

Емоційний вплив

Страх, цікавість, жадібність, довіра — емоційні тригери, що використовуються в соціотехнічних атаках.

3

Маніпулятивні техніки

Фрейминг, прийом «нога в дверях», імітація авторитету, створення ілюзії терміновості.

4

Захист від маніпуляцій

Критичне мислення, процедури верифікації, кібергігієна, підвищення обізнаності персоналу.

Лекційний матеріал (2 год.)

Психологія довіри та обману в контексті кібербезпеки. Принципи Чалдіні та їх застосування в соціотехнічних атаках: авторитет, взаємність, дефіцит, соціальний доказ, прихильність, послідовність. Когнітивні упередження та хибні евристики. Емоційні тригери атак. Психологічний портрет жертви та зловмисника. Поведінкові моделі безпеки користувачів ІКС.

Практичне заняття (1 год.) та СРС (5 год.)

Практика: Розбір реальних кейсів фішингових атак з виявленням використаних психологічних прийомів; тестування вразливості до маніпуляцій за стандартизованими методиками; дискусія «Чому технічний фахівець стає жертвою соціальної інженерії?».

СРС: Опрацювання: Гриценко В. С. «Кібербезпека: сучасні виклики та технології» (Київ: Юрінком Інтер, 2022) — розділ «Психологічні аспекти кіберзагроз»; підготовка аналітичної записки «Когнітивні упередження як вектор соціотехнічних атак».

МОДУЛЬ 1 · ТЕМА 1.3

Класифікація та типологія соціотехнічних атак

Лекційний матеріал (6 год., лекції 5–10)

Фішинг та його різновиди: масовий фішинг, спір-фішинг (spear phishing), китобійний фішинг (whaling), фармінг. Ознаки фішингових повідомлень. Інструменти виявлення та блокування.

Вішинг та смішинг: телефонні та SMS-атаки. Методи верифікації особистості. Захист від голосових маніпуляцій.

Бейтинг та претекстинг: використання фізичних носіїв, підроблені сценарії та легенди. Атаки на фізичний периметр безпеки (tailgating, piggybacking).

Інсайдерські загрози: типи інсайдерів, мотиви, індикатори підозрілої поведінки. APT-атаки з елементами соціальної інженерії.

Ключові питання

- Класифікація соціотехнічних атак за векторами та цілями
- Технічні та психологічні складові фішингових кампаній
- Різниця між масовими атаками та цільовими операціями
- Інсайдерська загроза: виявлення та запобігання
- APT-атаки та роль соціальної інженерії в них

Практичне заняття (2 год.)

Завдання 1. Аналіз зразків фішингових повідомлень: виявлення ознак атаки, психологічних прийомів, технічних індикаторів. Класифікація за типами.

Завдання 2. Кейс-стаді: розбір реального інциденту типу spear-phishing проти української організації. Реконструкція ланцюжка атаки.

Завдання 3. Тестування: визначення типу атаки за сценарієм (15 питань).

Самостійна робота (15 год.)

- Опрацювання: Бурячок В. Л. та ін. «Інформаційна та кібербезпека: соціотехнічний аспект» — розділи 2–3
- Підготовка презентації «Еволюція фішингових атак: від масового спаму до AI-фішингу»
- Складання класифікаційної схеми соціотехнічних атак з прикладами
- Аналіз звітів CERT-UA та Держспецзв'язку про соціотехнічні інциденти 2022–2024 рр.

Очікуваний результат: студент вміє класифікувати соціотехнічні атаки, описувати механізми їх реалізації та виявляти індикатори компрометації.

МОДУЛЬ 2

Методи виявлення та протидії соціотехнічним атакам

Тема 2.1

Технічні засоби виявлення та блокування соціотехнічних атак. Антифішинг, фільтрація пошти, багатофакторна автентифікація.

Тема 2.2

Організаційні заходи захисту. Політики безпеки, регламенти верифікації, програми підвищення обізнаності персоналу.

Тема 2.3

Тестування на проникнення (пентест) із застосуванням методів соціальної інженерії. Симуляції фішингових кампаній та оцінка рівня захищеності.

МОДУЛЬ 2 · ТЕМА 2.1

Технічні засоби виявлення та блокування атак

Лекційний матеріал (4 год., лекції 11–14)

Антифішингові технології: DNS-фільтрація, DMARC/DKIM/SPF-протоколи автентифікації електронної пошти, URL-аналізатори, браузерні розширення захисту. Системи виявлення та реагування на загрози (EDR/XDR).

Багатофакторна автентифікація (MFA): типи другого фактора, переваги та обмеження MFA у контексті соціотехнічних атак. Атаки на MFA: MFA-fatigue, SIM-swapping, атаки типу adversary-in-the-middle (AiTM).

SIEM та моніторинг поведінки: системи аналізу подій безпеки, поведінкова аналітика користувачів (UEBA), виявлення аномалій та індикаторів компрометації (IoC).

Захист від інсайдерів: DLP-системи (Data Loss Prevention), контроль привілейованого доступу (PAM), управління ідентифікацією та доступом (IAM/IGA).

Ключові питання

- Технічний стек захисту від фішингу та спуфінгу
- Роль MFA та її вразливості в контексті соціотехнічних атак
- SIEM та UEBA як інструменти виявлення інсайдерських загроз
- DLP-системи: принцип роботи та обмеження
- Інтеграція технічних засобів захисту в комплексну систему безпеки ІКС

Практичне заняття (2 год.)

Завдання 1. Налаштування та перевірка SPF/DKIM/DMARC-записів для навчального домену. Аналіз заголовків підозрілих email-повідомлень.

Завдання 2. Демонстрація роботи антифішингових інструментів: аналіз URL-адрес у пісочниці, перевірка IP-репутації, виявлення підроблених сертифікатів.

Завдання 3. Тестування: визначення ефективних технічних контрзаходів для заданих типів атак (10 сценаріїв).

Самостійна робота (10 год.)

- Опрацювання: Гриценко В. С. «Кібербезпека: сучасні виклики та технології» (Київ : Юрінком Інтер, 2022) — розділ «Технічні засоби захисту»
- Підготовка аналітичної записки «Атаки на MFA: методи та засоби протидії»
- Складання порівняльної таблиці антифішингових технологій та їх ефективності

Очікуваний результат: студент вміє описувати та порівнювати технічні засоби захисту від соціотехнічних атак, обґрунтовувати їх вибір для конкретних сценаріїв загроз.

МОДУЛЬ 2 · ТЕМА 2.2

Організаційні заходи захисту та політики безпеки

Оцінка ризиків

Ідентифікація активів, аналіз загроз, оцінка вразливостей людського фактора.

Розробка політик

Політики паролів, чистого столу, роботи з поштою, верифікації запитів.

Навчання персоналу

Програми обізнаності, регулярні тренінги, симуляції атак, тестування знань.

Процедури реагування

Плани реагування на інциденти, ескалація, звітування, аналіз після інциденту.

Аудит та контроль

Внутрішній аудит виконання політик, оцінка ефективності заходів захисту.

Лекційний матеріал (4 год., лекції 15–18)

Стратегія «людина-процес-технологія» в системі захисту від соціотехнічних атак. Розробка та впровадження організаційних політик безпеки. Програми підвищення обізнаності персоналу (Security Awareness Training): методи, інструменти, оцінка ефективності. Процедури верифікації запитів та ескалації підозрілих ситуацій. Культура безпеки в організації. Плани реагування на соціотехнічні інциденти (IRP). Управління ризиками, пов'язаними з людським фактором. Стандарти ISO 27001, NIST CSF у контексті організаційного захисту.

Практика (2 год.) та СРС (10 год.)

Практика: Розробка фрагменту політики інформаційної безпеки організації щодо протидії соціотехнічним атакам; складання плану програми Security Awareness Training для умовного підприємства; дискусія «Як виміряти ефективність навчання персоналу?».

СРС: Опрацювання: Кривоніс О. І. «Кібербезпека: правові та організаційні аспекти» (Київ : Центр навчальної літератури, 2022); підготовка аналітичної записки «Культура безпеки як основа організаційного захисту від соціотехнічних атак»; складання порівняльної таблиці вимог ISO 27001 та NIST CSF до організаційного захисту.

МОДУЛЬ 2 · ТЕМА 2.3

Пентест та симуляції соціотехнічних атак

Лекційний матеріал (2 год., лекція 19–20)

Тестування на проникнення (penetration testing) із застосуванням методів соціальної інженерії: мета, етика, правова база. Методологія соціотехнічного пентесту: розвідка (OSINT), підготовка легенди, реалізація атаки, звітування. OSINT-інструменти для збору інформації про ціль. Симуляції фішингових кампаній: платформи GoPhish, Gophish, KnowBe4. Red team / Blue team / Purple team підходи. Оцінка рівня захищеності організації від соціотехнічних атак. Звіт про пентест: структура, рекомендації, метрики.

Ключові питання

- Правові та етичні засади проведення соціотехнічного пентесту
- OSINT як інструмент розвідки в соціотехнічних атаках
- Методологія симуляції фішингових кампаній
- Метрики оцінки ефективності захисту
- Red/Blue/Purple team: ролі та взаємодія

Практичне заняття (2 год.)

Завдання 1. OSINT-розвідка проти навчального об'єкта (умовна організація): збір відкритих даних, складання профілю потенційної жертви, виявлення точок входу.

Завдання 2. Розробка сценарію симуляційної фішингової кампанії для умовної організації: мета, легенда, шаблон листа, критерії успіху.

Завдання 3. Підготовка та презентація фрагменту звіту про соціотехнічний пентест.

Самостійна робота (5 год.)

- Опрацювання: Ковальчук В. Ф. «Кіберзагрози та методи їх запобігання» (Львів : Галицькі контракти, 2022) — розділ «Тестування на проникнення»
- Підготовка аналітичної записки «OSINT-інструменти в арсеналі соціального інженера»
- Аналіз реальних кейсів Bug Bounty-програм, пов'язаних із соціальною інженерією

Очікуваний результат: студент вміє планувати симуляцію соціотехнічної атаки, застосовувати OSINT-методи та складати звіт про результати пентесту.

МОДУЛЬ 3

Правове регулювання та практика захисту в ІКС

Тема 3.1

Нормативно-правова база кібербезпеки України та міжнародні стандарти захисту від соціотехнічних загроз. Відповідальність за кіберзлочини.

Тема 3.2

Захист від соціотехнічних атак в критичній інфраструктурі та корпоративних ІКС. Кращі практики та галузеві стандарти.

Тема 3.3

Сучасні тенденції та майбутнє соціотехнічних загроз. AI-фішинг, діпфейки, автоматизована соціальна інженерія. Комплексний захист.

МОДУЛЬ 3 · ТЕМА 3.1

Нормативно-правова база кібербезпеки України

Лекційний матеріал (4 год., лекції 21–24)

Законодавство України у сфері кібербезпеки та захисту інформації: Закон «Про основні засади забезпечення кібербезпеки України» (2017), Закон «Про захист персональних даних», Кримінальна відповідальність за кіберзлочини (ст. 361–363 ККУ). Стратегія кібербезпеки України. Повноваження Держспецзв'язку, CERT-UA, Кіберполіції, СБУ. Міжнародні стандарти: ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-61, EU NIS2 Directive. GDPR та захист персональних даних у контексті соціотехнічних атак. Відповідальність організацій за інциденти кібербезпеки.

Ключові питання

- Правова база кібербезпеки України: ключові нормативні акти
- Кримінальна відповідальність за соціотехнічні атаки та кіберзлочини
- Роль державних органів у реагуванні на кіберінциденти
- Міжнародні стандарти та їх застосування в організаціях
- GDPR та захист персональних даних як об'єкта соціотехнічних атак

Практичне заняття (2 год.)

Завдання 1. Аналіз Закону України «Про основні засади забезпечення кібербезпеки України»: виявлення вимог до захисту від соціотехнічних загроз.

Завдання 2. Кейс: «Юридична відповідальність за соціотехнічну атаку — жертва чи організація?». Аналіз реального прецеденту з позицій українського законодавства.

Завдання 3. Порівняльна таблиця вимог ISO 27001 та NIS2 Directive щодо захисту від соціальної інженерії.

Самостійна робота (10 год.)

- Опрацювання: Кривоніс О. І. «Кібербезпека: правові та організаційні аспекти» (Київ : Центр навчальної літератури, 2022) — розділ «Правова база»
- Підготовка аналітичної записки «Стратегія кібербезпеки України: заходи проти соціотехнічних загроз»
- Аналіз статей 361–363 КК України у контексті кіберзлочинів із застосуванням соціальної інженерії

Очікуваний результат: студент вміє орієнтуватися в нормативно-правовій базі кібербезпеки, застосовувати вимоги законодавства та міжнародних стандартів до захисту від соціотехнічних загроз.

МОДУЛЬ 3 · ТЕМА 3.2

Захист від соціотехнічних атак в ІКС та критичній інфраструктурі

Ідентифікація та оцінка ризиків

Побудова моделі загроз для конкретної ІКС. Класифікація активів та визначення критичних точок впливу соціотехнічних атак.

Розробка та впровадження заходів

Технічні засоби + організаційні політики + навчання персоналу. Комплексний підхід до захисту критичної інфраструктури.

Моніторинг та реагування

Безперервний моніторинг, виявлення інцидентів, реагування за IRP, аналіз після інциденту та вдосконалення захисту.

Лекційний матеріал (4 год., лекції 25–28)

Галузева специфіка соціотехнічних атак: фінансовий сектор, критична інфраструктура, державні органи, IT-компанії. Реальні кейси атак на українські організації під час повномасштабного вторгнення. Комплексна система захисту від соціотехнічних загроз: Defense in Depth. Zero Trust Model та її застосування до людського фактора. Управління постачальниками та ланцюжком довіри (supply chain attacks). Програми MSSP та аутсорсинг безпеки.

Практика (2 год.) та СРС (10 год.)

Практика: Розробка комплексної моделі загроз для умовної ІКС; побудова матриці MITRE ATT&CK для соціотехнічних технік; дискусія «Zero Trust vs. Периметральна безпека у захисті від соціотехнічних атак».

СРС: Опрацювання: Ковальчук В. Ф. «Кіберзагрози та методи їх запобігання» (Львів : Галицькі контракти, 2022); підготовка аналітичної записки «Соціотехнічні атаки проти критичної інфраструктури України під час збройного конфлікту»; складання моделі загроз для реального підприємства за методологією STRIDE.

Очікуваний результат: студент вміє розробляти комплексну модель загроз, обирати відповідні контрзаходи та обґрунтовувати архітектуру захисту для конкретної ІКС.

МОДУЛЬ 3 · ТЕМА 3.3

Сучасні тенденції та майбутнє соціотехнічних загроз

Лекційний матеріал (2 год., лекції 29–30)

AI-фішинг та автоматизована генерація персоналізованих атак за допомогою великих мовних моделей (LLM). Діпфейки (deepfakes) у соціотехнічних атаках: відео, аудіо, синтетична особистість. Автоматизована соціальна інженерія (automated social engineering). Атаки на хмарні сервіси та SaaS-платформи через соціальну інженерію. Квантові загрози криптографії та пов'язані з ними ризики соціотехнічних атак. Розвиток регуляторного середовища: EU AI Act, NIS2. Тренди підготовки фахівців із кібербезпеки.

Ключові питання

- AI як інструмент соціальної інженерії нового покоління
- Діпфейки: загроза довірі та методи виявлення
- Захист від автоматизованих соціотехнічних атак
- Регуляторні відповіді на виклики AI-фішингу
- Перспективи розвитку соціотехнічної безпеки

Практичне заняття (2 год.)

Завдання 1. Аналіз прикладів AI-генерованих фішингових повідомлень: порівняння з традиційним фішингом, виявлення ознак автоматизації.

Завдання 2. Кейс: «Діпфейк-атака як інструмент CEO Fraud». Реконструкція сценарію, оцінка збитків, розробка контрзаходів.

Завдання 3. Захист міні-проектів: «Комплексна стратегія захисту умовної організації від сучасних соціотехнічних загроз».

Самостійна робота (10 год.)

- Опрацювання: Гриценко В. С. «Кібербезпека: сучасні виклики та технології» (Київ : Юрінком Інтер, 2022) — розділ «Штучний інтелект у кібербезпеці»
- Підготовка аналітичної записки «AI-фішинг: виклики та методи протидії для організацій»
- Аналіз вимог EU AI Act до AI-систем, що можуть використовуватися в соціотехнічних атаках

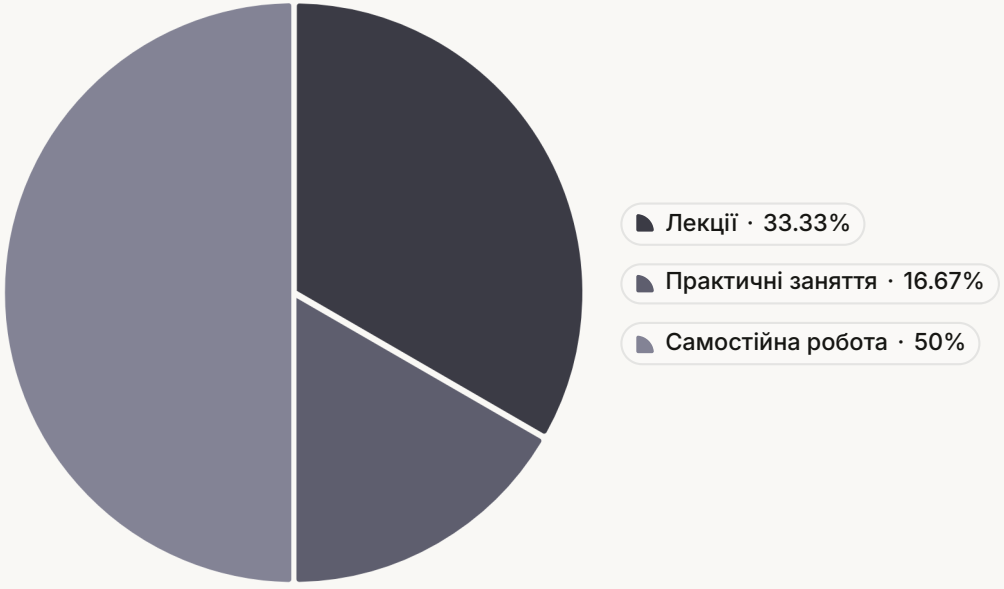
Очікуваний результат: студент вміє прогнозувати тенденції розвитку соціотехнічних загроз, оцінювати вплив AI та діпфейків на безпеку ІКС та розробляти перспективні заходи захисту.

Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Соціотехнічна безпека. Людський фактор	4	1	5
	Тема 1.2 — Психологічні основи соціальної інженерії	2	1	5
	Тема 1.3 — Класифікація соціотехнічних атак	6	2	15
Модуль 2	Тема 2.1 — Технічні засоби виявлення та блокування	4	2	10
	Тема 2.2 — Організаційні заходи захисту та політики безпеки	4	2	10
	Тема 2.3 — Пентест та симуляції соціотехнічних атак	2	2	5
Модуль 3	Тема 3.1 — Нормативно-правова база кібербезпеки	4	2	10
	Тема 3.2 — Захист ІКС та критичної інфраструктури	4	2	10
	Тема 3.3 — Сучасні тенденції та AI-загрози	2	2	10
Разом	**3 модулі, 9 тем**	**30**	**15**	**45**

Загальний обсяг: 90 годин = 3 кредити ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

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

Лекції — 30 год. (33%)

Системне подання ключового теоретичного матеріалу з використанням наочних схем, таблиць, розбору реальних інцидентів та прикладів кіберзагроз.

Практичні — 15 год. (17%)

Відпрацювання навичок виявлення атак, аналіз фішингових зразків, розробка сценаріїв захисту, захист міні-проектів із соціотехнічної безпеки.

Самостійна робота — 45 год. (50%)

Поглиблене вивчення, підготовка аналітичних записок, робота з нормативними документами, науковою літературою та звітами CERT-UA. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками з соціотехнічної безпеки та кібербезпеки (Бурячок, Гриценко, Кривоніс, Ковальчук та ін.), нормативно-правовими актами, науковими статтями у фахових виданнях. Студент конспектує ключові положення, виділяє головні поняття та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (аналіз інцидентів, складання моделей загроз, оцінка ризиків); творчих завдань — аналітичні записки, реферати, міні-дослідження з питань соціотехнічної безпеки та захисту інформаційно-комунікаційних систем.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: CERT-UA (**cert.gov.ua**), Держспецзв'язку (**cip.gov.ua**), Кіберполіції (**cyberpolice.gov.ua**), Верховної Ради (**zakon.rada.gov.ua**). Аналіз звітів CERT-UA, бюлетенів кіберзагроз для підготовки навчальних завдань.

Підготовка до занять

Підготовка до практичних занять (опрацювання кейсів, повторення теорії атак); підготовка до тестувань (ключові терміни, класифікації, нормативна база); підготовка до контрольних робіт за кожним модулем (систематизація знань, типові сценарії).

Форми контролю знань

1	2	3
Поточний контроль	**Проміжний контроль**	**Підсумковий контроль**
Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість аналізу інцидентів і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Проводиться після кожної теми у формі тестування (10–15 питань) або усного опитування.	Самостійна робота — комплексне ситуаційне завдання або аналітична записка, що охоплює теми змістовного модуля (аналіз загроз, розробка моделі атаки та захисту, нормативні вимоги). Оцінюються повнота відповіді, аргументованість, технічна коректність та обґрунтованість висновків. Проводиться після завершення кожного змістовного модуля.	Залік відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання. 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 «Соціотехнічна безпека» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок виявлення та протидії соціотехнічним атакам, необхідних для майбутньої професійної діяльності у сфері захисту інформації в ІКС.

Лекції

Системне подання теоретичного матеріалу з демонстрацією реальних прикладів атак, схем, технічних діаграм; студенти ведуть конспекти та ставлять аналітичні запитання.

Аналіз інцидентів

Опрацювання реальних кейсів соціотехнічних атак; формування навичок реконструкції ланцюжка атаки, оцінки наслідків та розробки контрзаходів.

Кейс-стади

Аналіз реальних ситуацій соціотехнічних атак; студенти виявляють вразливості, пропонують захисні заходи та обґрунтовують висновки на основі нормативних вимог.

Дискусії

Обговорення дискусійних питань кібербезпеки та соціотехнічних загроз; розвиток критичного мислення, аргументації та здатності обґрунтовувати технічні рішення.

Самостійне дослідження

Підготовка аналітичних записок, рефератів і презентацій з питань соціотехнічної безпеки; розвиток навичок самостійного пошуку та аналізу актуальних загроз.

Симуляційні вправи

Практичне виконання OSINT-розвідки, аналіз фішингових зразків, розробка сценаріїв атак і захисних заходів; формування практичних компетентностей у захисті ІКС.

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

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

1. Гриценко В. С.
Кібербезпека: сучасні виклики та технології. — Київ : Юрінком Інтер, 2022. — 384 с.

2. Кривоніс О. І.
Кібербезпека: правові та організаційні аспекти : навч. посіб. — Київ : Центр навчальної літератури, 2022. — 310 с.

3. Ковальчук В. Ф.
Кіберзагрози та методи їх запобігання. — Львів : Видавничий дім «Галицькі контракти», 2022. — 272 с.

4. Пашорін В. І., Костюк Ю. В.
Кібербезпека: ключові питання : навч. посіб. — Київ : ДТЕУ, 2023. — 245 с.

5. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.
Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. проф. В. Б. Толубка. — Київ : ДУТ, 2015 (рекомендовано для тем 1.1–1.3). — 288 с.

6. Сілін Є. С., Кадубовський О. А.
Основи кібербезпеки : навч. посіб. — Київ, 2023. — 198 с.

7. Терновий О., Шкуренко О., Міненко Л.
Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України. Сучасні інформаційні технології у сфері безпеки та оборони. — 2023. — № 46(1). — С. 23–31.

8. Крижанівська Т., Коршун Н.
Соціотехнічні атаки: типи, характеристики та методи протидії. Безпека інформаційно-комунікаційних систем. — 2025. — № 1. — С. 12–22.

Додаткова література та наукові статті

9. Ганченко М. О.

Соціальна інженерія як засіб отримання таємної інформації: аналіз методів та заходи захисту. — Київ : ДУІКТ, 2022. — 148 с. *Рекомендується для тем 1.2–1.3 (психологічні основи та класифікація атак).*

10. Єршова О. О., Гончаренко І. М.

Сучасні моделі управління захистом інформації в умовах кіберзагроз. Журнал стратегічних економічних досліджень. — 2022. — № 2(7). — С. 75–84. *Рекомендується для тем 2.2–3.2.*

11. Крижанівська Т. О.

Соціотехнічні атаки: моделювання, симуляція та реалізація методів захисту. Телекомунікаційні та інформаційні технології. — 2026. — № 1. — С. 90–113. *Рекомендується для теми 2.3 (пентест).*

12. Турченко Ф. Г., Панченко П. П.

Управління ризиками кібербезпеки в організаціях: підручник для ЗВО. — 2-ге вид., перероб. — Київ : Генеза, 2022. — 312 с. *Рекомендується для модулів 2–3.*

Нормативно-правова база

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

  Визначає правові та організаційні засади забезпечення кібербезпеки України, захисту критичної інфраструктури. **zakon.rada.gov.ua**

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

  Регулює відносини у сфері захисту інформації, що обробляється в ІКС. **zakon.rada.gov.ua**

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

  Регулює правовідносини, пов'язані із захистом персональних даних — основного об'єкта соціотехнічних атак. **zakon.rada.gov.ua**

- Кримінальний кодекс України, статті 361–363

  Кримінальна відповідальність за несанкціонований доступ до комп'ютерних систем, перехоплення даних та кіберзлочини. **zakon.rada.gov.ua**

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

  Визначає пріоритети державної політики у сфері кібербезпеки на 2021–2025 рр. **zakon.rada.gov.ua**

Офіційні ресурси та фахові видання

CERT-UA

cert.gov.ua — Урядова команда реагування на комп'ютерні надзвичайні події: бюлетені загроз, аналіз інцидентів, рекомендації із захисту від соціотехнічних атак.

Держспецзв'язку

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

Кіберполіція України

cyberpolice.gov.ua — матеріали про кіберзлочини, інформування про соціотехнічні шахрайства, статистика інцидентів.

Верховна Рада України

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

Журнал «Кібербезпека: освіта, наука, техніка»

csecurity.kubg.edu.ua — провідне українське фахове видання з питань кібербезпеки та захисту інформаційних систем.

Журнал «Безпека інформаційно-комунікаційних систем»

elibrary.kubg.edu.ua — наукові статті з питань захисту ІКС, соціотехнічної безпеки та кіберзагроз.

Національна бібліотека ім. В. І. Вернадського

nbuv.gov.ua — електронні ресурси, наукові статті, монографії з кібербезпеки та захисту інформації.

Міністерство освіти і науки України

mon.gov.ua — освітні стандарти, навчальні програми зі спеціальності 123 «Комп'ютерна інженерія».

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

Чому «Соціотехнічна безпека» для інженерів?

Дисципліна «Соціотехнічна безпека» є невід'ємною складовою підготовки бакалаврів зі спеціальністю 123 «Комп'ютерна інженерія» за програмою «Організація захисту інформації в ІКС». Розуміння соціотехнічних загроз формує у майбутніх інженерів здатність проектувати системи захисту, що враховують людський фактор як ключову вразливість.

Сучасний фахівець у сфері захисту інформації повинен розуміти, що 80–90% успішних кібератак розпочинаються із соціотехнічного вектора — тому технічний захист без захисту людського фактора є неповним.

Практичне значення для майбутньої кар'єри

- Здатність проектувати комплексні системи захисту ІКС з урахуванням людського фактора
- Навички проведення оцінки ризиків та аудиту безпеки організацій
- Компетентність у розробці та впровадженні програм підвищення обізнаності персоналу
- Знання правової бази для роботи в сфері захисту інформації та кібербезпеки
- Практичні навички OSINT та соціотехнічного пентесту
- Готовність до реагування на соціотехнічні інциденти в реальних ІКС

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові аспекти соціотехнічної безпеки — від природи психологічних маніпуляцій до сучасних AI-загроз — і формує у студентів цілісне розуміння захисту інформаційно-комунікаційних систем від людськоорієнтованих кібератак.

Бажаємо успіхів у вивченні Соціотехнічної безпеки!

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

9

Тем

У 3 змістовних модулях

8

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Найслабша ланка в системі безпеки — це людина. Найсильніша — теж людина.» — Кевін Митнік

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