Силабус дисципліни «Соціотехнічна безпека»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР

90 Годин загальний обсяг дисципліни	3 Кредити ЄКТС відповідно до стандарту
3 Змістовних модулі 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 курсу

Мета дисципліни

Дисципліна «Соціотехнічна безпека» формує у студентів спеціальності «Комп'ютерна інженерія» системне розуміння природи соціотехнічних загроз, методів соціальної інженерії та механізмів захисту від них в інформаційно-комунікаційних системах. Курс спрямований на розвиток критичного мислення щодо людського чинника в кібербезпеці, вміння виявляти та нейтралізувати атаки соціальної інженерії, а також на формування культури безпеки в організаціях.

Форми навчання

- Лекції — 30 годин
- Практичні заняття — 15 годин
- Самостійна робота — 45 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання інформації у контексті забезпечення інформаційної безпеки: виявлення соціотехнічних загроз, порівняння методів атак і захисних заходів, формування обґрунтованих висновків та прийняття рішень. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань із захисту інформаційних систем від соціотехнічних атак.

Здатність до усної та письмової комунікації в контексті інформаційної безпеки: чітко пояснювати поняття соціотехнічних загроз, аргументовано обґрунтовувати вибір засобів захисту, оформлювати звіти та аналітичні матеріали. Відповідальність, ініціативність та готовність працювати в команді під час проведення аудитів безпеки та пентестів.

- Аналізувати соціотехнічні загрози та вектори атак
- Виділяти головне та узагальнювати результати аналізу безпеки
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися з викладачами та одногрупниками
- Брати участь у командній роботі при проведенні тестувань на проникнення

Фахові компетентності

Розуміння сутності та механізмів соціотехнічних атак, їхньої класифікації, методів соціальної інженерії та психологічних принципів, які використовуються зловмисниками для маніпулювання людьми з метою несанкціонованого доступу до інформаційних систем.

Здатність застосовувати методи виявлення, аналізу та протидії соціотехнічним атакам в інформаційно-комунікаційних системах; розробляти та впроваджувати організаційні заходи захисту; проводити навчання персоналу з питань кібергігієни та безпечної поведінки в цифровому середовищі.

- Класифікувати соціотехнічні атаки та загрози
- Аналізувати вразливості людського чинника в ІКС
- Розробляти заходи протидії соціальній інженерії
- Проводити тестування соціотехнічної захищеності організацій
- Формувати корпоративну культуру кібербезпеки

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових категорій та явищ: соціотехнічна атака, соціальна інженерія, фішинг, претекстинг, вішинг, тейлгейтинг, людський чинник у кібербезпеці, культура безпеки. Характеризувати основні класи соціотехнічних загроз та психологічні механізми, що лежать в їх основі.

2

Аналіз та оцінювання

Аналізувати причини успішності соціотехнічних атак, виявляти вразливості людського чинника в конкретних організаціях. Оцінювати ефективність заходів захисту від соціальної інженерії, порівнювати різні підходи до формування культури безпеки.

3

Застосування знань

Застосовувати методи тестування соціотехнічної захищеності організацій, розробляти сценарії атак для цілей аудиту безпеки. Використовувати нормативно-правову базу та стандарти для побудови системи захисту від соціотехнічних загроз в ІКС.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо вибору засобів захисту від соціотехнічних атак. Формувати відповідальне ставлення до інформаційної безпеки та культуру безпечної поведінки у цифровому середовищі.

Модуль 1. Основи соціотехнічної безпеки та людський чинник

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Вступ до соціотехнічної безпеки. Поняття «соціотехнічна система», «соціотехнічна безпека» та «соціотехнічна атака». Місце людського чинника в системі інформаційної безпеки. Класифікація соціотехнічних загроз. Статистика та тенденції соціотехнічних атак в Україні та світі.

Тема 1.2

Психологічні засади соціальної інженерії. Психологічні принципи впливу на людину: авторитет, терміновість, взаємність, соціальний доказ, дефіцит, прихильність. Когнітивні упередження та їх використання в атаках. Маніпулятивні техніки та методи переконання.

Тема 1.3

Нормативно-правове регулювання. Законодавство України у сфері інформаційної та кібербезпеки. Закони «Про інформацію», «Про кібербезпеку», «Про захист персональних даних». Стандарти ISO/IEC 27001, NIST. Відповідальність за злочини у сфері IT.

Тема 1.4

Організаційні засади захисту. Поняття політики інформаційної безпеки. Роль персоналу як «слабкої ланки» захисту. Модель управління ризиками соціотехнічних атак. Класифікація потенційних зловмисників: зовнішні та внутрішні загрози (інсайдери).

Модуль 2. Методи та техніки соціотехнічних атак

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Фішинг та його різновиди. Класичний фішинг, спір-фішинг, вейлінг, клон-фішинг. Вішинг (голосовий фішинг) та смішинг (SMS-фішинг). Фішингові кампанії: структура, інструменти, інфраструктура. Методи виявлення та протидії фішинговим атакам.

Тема 2.2

Претекстинг та імперсонація. Метод претекстингу: розробка та відпрацювання легенди. Імперсонація (видавання себе за іншу особу): онлайн та офлайн. Збір OSINT-інформації для підготовки атаки. Атаки через соціальні мережі та месенджери. Baiting та quid pro quo.

Тема 2.3

Фізичні соціотехнічні атаки. Тейлгейтинг (несанкціоноване проходження). Підглядання (shoulder surfing). Атаки через залишені носії інформації (USB drops). Атаки на фізичну інфраструктуру. Dumpster diving (перегляд сміття). Методи захисту від фізичних атак.

Модуль 3. Протидія соціотехнічним атакам та культура безпеки

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Тестування соціотехнічної захищеності. Пентест соціальної інженерії: цілі, методологія, етапи. Розробка сценаріїв атак для аудиту. Інструменти для проведення соціотехнічних тестів: SET (Social Engineering Toolkit), GoPhish. Оформлення звіту за результатами тестування. Етичні та правові аспекти пентесту.

Тема 3.2

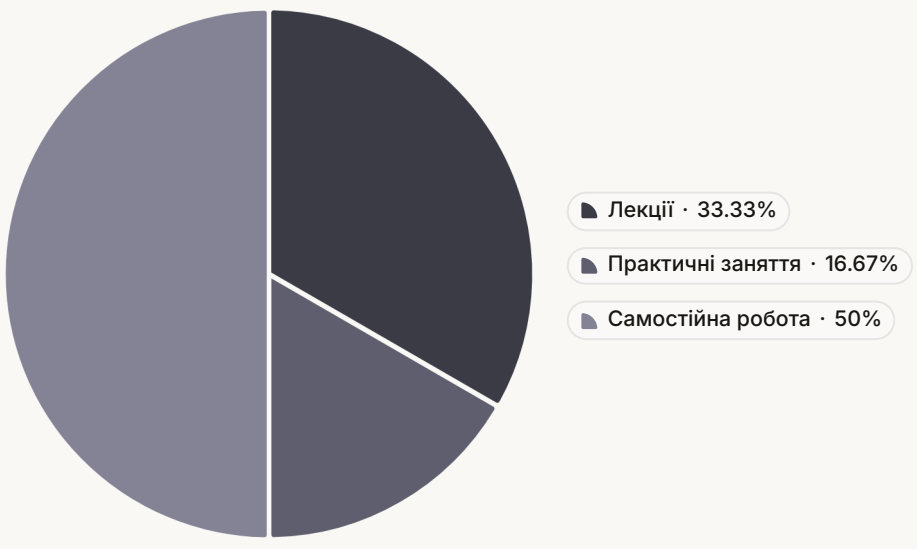
Технічні засоби протидії. Антифішингові засоби захисту: фільтри електронної пошти, DMARC/SPF/DKIM. Багатофакторна автентифікація як захист від компрометації облікових даних. Системи виявлення аномалій поведінки (UEBA). DLP-системи для протидії інсайдерським загрозам. Засоби моніторингу та реагування на інциденти.

Тема 3.3

Формування культури кібербезпеки. Програми підвищення обізнаності персоналу з питань безпеки (Security Awareness Training). Розробка навчальних матеріалів та тренінгів. Симуляційні фішингові кампанії для навчання. Метрики оцінки ефективності навчання. Побудова корпоративної культури безпеки в організаціях захисту ІКС.

Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Вступ до соціотехнічної безпеки	2	2	4
	Тема 1.2 — Психологічні засади соціальної інженерії	4	2	5
	Тема 1.3 — Нормативно-правове регулювання	2	2	4
	Тема 1.4 — Організаційні засади захисту	2	1	4
Модуль 2	Тема 2.1 — Фішинг та його різновиди	4	2	6
	Тема 2.2 — Претекстинг та імперсонація	4	2	6
	Тема 2.3 — Фізичні соціотехнічні атаки	4	2	6
Модуль 3	Тема 3.1 — Тестування соціотехнічної захищеності	4	2	6
	Тема 3.2 — Технічні засоби протидії	2	0	5
	Тема 3.3 — Формування культури кібербезпеки	2	0	5
Разом		**30**	**15**	**45**



Структура навчального часу

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

- **Лекції (30 год. — 33%):** подача ключового теоретичного матеріалу
- **Практичні (15 год. — 17%):** відпрацювання навичок, аналіз кейсів, симуляція атак
- **Самостійна робота (45 год. — 50%):** поглиблене вивчення, підготовка завдань

Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються самостійно аналізувати реальні кейси соціотехнічних атак.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками з соціотехнічної безпеки та кібербезпеки, нормативно-правовими актами, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до класифікації соціотехнічних атак.

Індивідуальні завдання

Виконання аналітичних завдань щодо розбору реальних інцидентів соціотехнічних атак, підготовка есе, аналітичних записок, міні-досліджень з актуальних питань кіберзагроз. Моделювання сценаріїв атак та розробка заходів протидії для конкретних організацій.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: CERT-UA (**cert.gov.ua**), Держспецзв'язку (**cip.gov.ua**), ДЦКЗ (**ncscc.gov.ua**). Аналіз публічних звітів про кіберінциденти, пошук актуальної інформації про нові вектори атак.

Підготовка до занять

Підготовка до практичних занять шляхом опрацювання першоджерел, повторення теоретичного матеріалу; підготовка до тестувань через вивчення ключових термінів і визначень; систематизація знань перед контрольними роботами.

Методи викладання

→ Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць класифікації атак і реальних прикладів із практики; студенти ведуть конспекти та ставлять уточнювальні запитання.

→ Кейс-стаді

Аналіз реальних інцидентів соціотехнічних атак на організації; студенти виявляють вектори атак, пропонують заходи захисту та обґрунтовують висновки на основі актуальних даних.

→ Рольові ігри та симуляції

Моделювання сценаріїв соціотехнічних атак: студенти виступають у ролі як зловмисників, так і захисників; розвиток практичних навичок виявлення та нейтралізації загроз.

→ Практичні лабораторні

Робота з інструментами тестування соціотехнічної захищеності (SET, GoPhish); формування навичок розробки фішингових симуляцій та аналізу їхніх результатів.

→ Самостійне дослідження

Підготовка аналітичних звітів про реальні соціотехнічні атаки та рефератів за обраною темою; розвиток навичок самостійного пошуку та систематизації інформації.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість аналізу соціотехнічних загроз і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові відповіді на запитання, аналіз кейсів та участь у практичних симуляціях.

2

Проміжний контроль

Самостійна робота — комплексне ситуаційне завдання або реферат, які охоплюють теми змістовних модулів (теоретичні питання, аналіз інцидентів, розробка заходів протидії соціотехнічним атакам). Оцінюються повнота відповіді, правильність аналізу та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Іспит 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 оцінювання: 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 «Організація захисту інформації в інформаційно-комунікаційних системах» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. — Львів : Магнолія 2006, 2024. — 288 с.
2. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: монографія / за заг. ред. проф. Ю. Г. Даника. — Житомир : ЖНАЕУ, 2022. — 636 с.
3. Опірський І. Р. Методи та засоби захисту інформації в комп'ютерних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
4. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2023. — 248 с.
5. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. Інформаційна безпека: підручник / під ред. В. В. Остроухова. — Київ : Ліра-К, 2022. — 412 с.
6. Ткач Ю. М., Шелест М. Є., Хорошко В. О., Дюба І. М. Захист кіберпростору: монографія. — Чернігів : НУЧП, 2023. — 292 с.
7. Бобало Ю. Я. та ін. Інформаційна безпека: навч. посіб. / за заг. ред. Ю. Я. Бобала та І. В. Горбатого. — Львів : Видавництво Львівської політехніки, 2022. — 580 с.
8. Сілін Є. С., Кадубовський О. А. Основи кібербезпеки: соціальна інженерія: навч. посіб. — Дніпро : ДДУВС, 2023. — 180 с.
9. Голіков Ю. М., Острянська Є. В. Штучний інтелект та кібербезпека: нові виклики / Комп'ютерні науки та кібербезпека. — Харків : ХНУ ім. Каразіна, 2024. — № 2 (26). — С. 45–58.
10. Довгань О. Д., Литвинова Л. А. Кібербезпека: дайджест актуальних загроз. — Київ : НДІ інформатики і права НАПрН України, 2023. — 316 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події. — URL: **https://cert.gov.ua/**
3. Національний координаційний центр кібербезпеки. — URL: **https://ncscc.gov.ua/**
4. Офіційний сайт Верховної Ради України (законодавство). — URL: **https://zakon.rada.gov.ua/**
5. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
6. Науково-дослідний інститут інформатики і права НАПрН України (журнал «Кібербезпека»). — URL: **https://ippi.org.ua/**
7. Журнал «Комп'ютерні науки та кібербезпека» (ХНУ ім. Каразіна). — URL: **https://periodicals.karazin.ua/cscs**
8. Науковий журнал «Захист інформації» (НАУ). — URL: **https://jrnl.nau.edu.ua/index.php/ZI**

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