Силабус дисципліни «Інформаційна та кібербезпека сучасного підприємства»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР · ОП «ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС»

120

Годин загальний обсяг дисципліни

4

Кредити ЄКТС відповідно до стандарту

4

Змістовних модулі курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Інформаційна та кібербезпека сучасного підприємства

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки курсу

Мета дисципліни

Дисципліна «Інформаційна та кібербезпека сучасного підприємства» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері забезпечення інформаційної та кібербезпеки підприємств та організацій. Курс спрямований на опанування концептуальних основ захисту інформації, методів виявлення та нейтралізації кіберзагроз, принципів побудови комплексних систем захисту інформації на підприємстві, а також сучасних стандартів і нормативно-правових вимог у сфері кібербезпеки в умовах цифрової трансформації та воєнного стану.

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 та кібербезпеки: виявлення актуальних загроз, порівняння підходів до захисту, формування обґрунтованих висновків щодо організації безпеки підприємства. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки аналітичних матеріалів, технічних звітів та планів захисту.

Здатність до усної та письмової фахової комунікації: чітко пояснювати вимоги нормативних документів, аргументовано обґрунтовувати рішення щодо захисту інформаційних ресурсів підприємства. Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді під час виконання практичних завдань.

- Аналізувати нормативно-правові акти у сфері кібербезпеки та захисту інформації
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися з викладачами та одногрупниками
- Брати участь у командній роботі та розподіляти обов'язки

Фахові компетентності

Розуміння сутності та закономірностей організації інформаційної та кібербезпеки підприємства, її місця в системі захисту інформації в інформаційно-комунікаційних системах. Знання ключових понять, нормативних вимог і технічних засобів захисту корпоративних інформаційних ресурсів, уміння застосовувати їх у практичній діяльності фахівця з інформаційної безпеки.

Здатність застосовувати методи та засоби захисту інформаційних систем підприємства для забезпечення конфіденційності, цілісності та доступності інформації, зокрема в умовах хмарних технологій, кіберзагроз та цифрової трансформації.

- Характеризувати нормативно-правову базу кібербезпеки підприємства
- Виявляти та класифікувати кіберзагрози і вразливості ІС підприємства
- Застосовувати технічні та організаційні заходи захисту від кібератак
- Організовувати систему управління інцидентами кібербезпеки
- Проводити аудит та оцінку ризиків інформаційної безпеки підприємства

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять інформаційної та кібербезпеки підприємства: кіберзагроза, кіберінцидент, кіберризик, вразливість, несанкціонований доступ, комплексна система захисту інформації, політика безпеки. Характеризувати нормативно-правову базу та міжнародні стандарти (ISO/IEC 27001, NIST CSF), що регламентують організацію кібербезпеки на підприємствах в Україні.

2

Аналіз та оцінювання

Аналізувати інформаційні системи підприємства з точки зору вимог кібербезпеки, виявляти вразливості та загрози. Оцінювати ризики інформаційної безпеки, визначати пріоритети захисних заходів та відповідність систем захисту вимогам чинного законодавства й галузевих стандартів.

3

Застосування знань

Застосовувати методи та засоби захисту інформаційних ресурсів підприємства від кіберзагроз. Розробляти політики безпеки, плани реагування на інциденти, налаштовувати засоби технічного захисту в корпоративних мережах та хмарних середовищах.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо організації кібербезпеки підприємства в конкретних умовах функціонування ІКС. Формувати професійну відповідальність і розуміння важливості дотримання режиму кібербезпеки у фаховій діяльності в умовах цифрових трансформацій та кіберзагроз воєнного часу.

Модуль 1. Концептуальні та нормативно-правові основи кібербезпеки підприємства

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Поняття та сутність інформаційної та кібербезпеки підприємства. Місце кібербезпеки в системі безпеки сучасного підприємства. Основні терміни та визначення: кіберпростір, кібербезпека, кіберзагроза, кіберінцидент, інформаційна безпека. Класифікація активів підприємства та їх цінність. Принципи CIA-тріади у корпоративному середовищі.

Тема 1.2

Нормативно-правова та стандартизаційна база кібербезпеки. Закони України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних». Стратегія кібербезпеки України. Міжнародні стандарти ISO/IEC 27001, 27002, NIST CSF, CIS Controls.

Тема 1.3

Кіберзагрози та вразливості інформаційних систем підприємства. Класифікація кіберзагроз і кібератак. Зловмисне програмне забезпечення: віруси, трояни, ransomware, spyware. Соціальна інженерія та фішинг. Вразливості корпоративних мереж та застосунків. Актуальний ландшафт кіберзагроз в умовах воєнного стану.

Тема 1.4

Оцінка ризиків інформаційної безпеки підприємства. Поняття ризику інформаційної безпеки. Методології оцінки ризиків: OCTAVE, CRAMM, ISO/IEC 27005. Ідентифікація активів, загроз та вразливостей. Кількісні та якісні методи оцінки ризиків. Розробка плану обробки ризиків підприємства.

Модуль 2. Технічні засоби та методи захисту інформаційних систем підприємства

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Захист мережевої інфраструктури підприємства. Архітектура корпоративної мережі з точки зору безпеки. Міжмережеві екрани (Firewall) та системи виявлення/запобігання вторгненням (IDS/IPS). Сегментація мережі та DMZ. VPN та шифрування трафіку. Захист бездротових мереж підприємства. Моніторинг мережевої активності.

Тема 2.2

Управління доступом та ідентифікація в корпоративних системах. Принципи управління доступом: дискреційна, мандатна, рольова моделі. Системи автентифікації та авторизації. Багатофакторна автентифікація (MFA). Управління привілейованим доступом (PAM). Каталогові служби: Active Directory, LDAP. Zero Trust архітектура.

Тема 2.3

Криптографічний захист інформації на підприємстві. Основи симетричного та асиметричного шифрування у корпоративних застосуваннях. Інфраструктура відкритих ключів (PKI) підприємства. Електронний цифровий підпис. Шифрування баз даних та файлових систем. Захист електронної пошти та корпоративних комунікацій.

Модуль 3. Організаційне забезпечення кібербезпеки та управління інцидентами

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Система управління інформаційною безпекою підприємства (СУІБ). Концепція СУІБ за ISO/IEC 27001. Цикл PDCA в управлінні безпекою. Організаційна структура підрозділу з кібербезпеки. Політики та процедури безпеки. Класифікація інформаційних активів підприємства. Програма підвищення обізнаності персоналу з кібербезпеки.

Тема 3.2

Управління інцидентами кібербезпеки на підприємстві. Поняття кіберінциденту та класифікація. Процес виявлення, реєстрації та класифікації інцидентів. Реагування на інциденти: стримування, знищення, відновлення. SOC (Security Operations Center): функції та інструменти. SIEM-системи для моніторингу інцидентів. Форензика та розслідування кіберінцидентів.

Тема 3.3

Забезпечення безперервності бізнесу та відновлення після кіберінцидентів. BCP (Business Continuity Plan) та DRP (Disaster Recovery Plan). Резервне копіювання та відновлення даних. RTO та RPO як показники відновлення. Стійкість до ransomware-атак. Тестування планів відновлення. Особливості забезпечення безперервності в умовах гібридної війни.

Модуль 4. Кібербезпека в сучасних середовищах та аудит

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Кібербезпека хмарних середовищ та IoT на підприємстві. Моделі хмарних послуг (IaaS, PaaS, SaaS) та їх безпека. Спільна відповідальність за безпеку в хмарі. Захист хмарних застосунків та зберігання даних. Безпека Інтернету речей (IoT) в корпоративному середовищі. Промислові системи управління (ICS/SCADA) та їх захист.

Тема 4.2

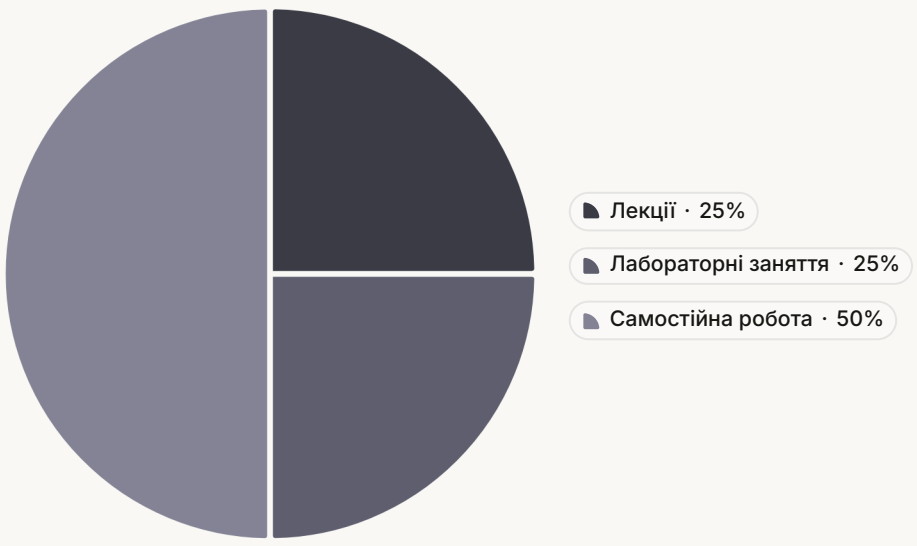
Захист об'єктів критичної інфраструктури та корпоративних даних. Поняття критичної інформаційної інфраструктури (КІІ). Категорії об'єктів КІІ в Україні. Захист персональних даних відповідно до законодавства. Data Loss Prevention (DLP) рішення. Безпека баз даних підприємства. Захист від APT-атак та цілеспрямованого кібершпигунства.

Тема 4.3

Аудит та тестування кібербезпеки підприємства. Аудит інформаційної безпеки: цілі, методи, стандарти. Пентестинг (тестування на проникнення): методологія та інструменти. Сканування вразливостей корпоративних систем. Аудит відповідності вимогам ISO 27001. Звітування за результатами аудиту кібербезпеки. Актуальні виклики аудиту в умовах воєнного стану.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	Самостійна робота (год.)	Разом
Модуль 1	Тема 1.1 — Поняття та сутність кібербезпеки підприємства	2	2	4	8
	Тема 1.2 — Нормативно-правова та стандартизаційна база	2	2	4	8
	Тема 1.3 — Кіберзагрози та вразливості ІС підприємства	2	2	4	8
	Тема 1.4 — Оцінка ризиків інформаційної безпеки	2	2	4	8
Модуль 2	Тема 2.1 — Захист мережевої інфраструктури	2	4	6	12
	Тема 2.2 — Управління доступом та ідентифікація	2	4	6	12
	Тема 2.3 — Криптографічний захист інформації	2	4	6	12
Модуль 3	Тема 3.1 — Система управління інформаційною безпекою (СУІБ)	4	2	6	12
	Тема 3.2 — Управління інцидентами кібербезпеки	4	4	6	14
	Тема 3.3 — Безперервність бізнесу та відновлення після інцидентів	2	2	6	10
Модуль 4	Тема 4.1 — Кібербезпека хмарних середовищ та IoT	2	2	6	10
	Тема 4.2 — Захист КІІ та корпоративних даних	2	0	6	8
	Тема 4.3 — Аудит та тестування кібербезпеки підприємства	2	2	6	10
Разом		**30**	**30**	**60**	**120**



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 з кібербезпеки підприємства
- **Лабораторні (30 год. — 25%):** практичне відпрацювання навичок налаштування засобів захисту, аналіз кіберзагроз, вирішення кейсів
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, підготовка завдань, аналіз стандартів

Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються самостійно опрацьовувати нормативні документи, стандарти кібербезпеки та технічну документацію.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з кібербезпеки та захисту інформації, нормативно-правовими актами, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до організації кібербезпеки підприємства.

Індивідуальні завдання

Виконання аналітичних завдань щодо оцінки ризиків, розробки моделі загроз для умовного підприємства, підготовка політик безпеки, планів реагування на інциденти, аналітичних записок з актуальних питань кібербезпеки в умовах цифрової трансформації.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), CERT-UA (**cert.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**). Аналіз бюлетенів кіберзагроз, рекомендацій щодо захисту від актуальних кібератак, стандартів ISO серії 27000.

Підготовка до лабораторних

Підготовка до лабораторних занять шляхом опрацювання технічної документації, вивчення інструментів кібербезпеки (Nmap, Wireshark, Metasploit, OpenVAS); підготовка до тестувань через вивчення ключових термінів та понять; систематизація знань перед контрольними роботами.

Методи викладання

→ Лекції

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

→ Кейс-стаді

Аналіз реальних кіберінцидентів та кібератак на українські підприємства; студенти виявляють вектор атаки, пропонують заходи захисту та обґрунтовують висновки.

→ Лабораторні роботи

Практичне налаштування засобів захисту: фаєрволів, IDS/IPS, VPN; сканування вразливостей; аналіз мережевого трафіку; тестування систем на проникнення у контрольованому середовищі.

→ Робота зі стандартами

Опрацювання міжнародних та національних стандартів кібербезпеки (ISO 27001, NIST); формування навичок аналізу нормативно-правового та стандартизаційного середовища та їх практичного застосування.

→ Самостійне дослідження

Підготовка аналітичних записок, рефератів і презентацій за обраною темою кібербезпеки; розвиток навичок самостійного пошуку та систематизації нормативної й технічної інформації.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість відповідей і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові відповіді на запитання, захист лабораторних робіт та участь у вирішенні кейсів із кібербезпеки підприємства.

2

Проміжний контроль

Самостійна робота — комплексне практичне завдання або реферат, які охоплюють теми змістовних модулів (теоретичні питання, аналіз нормативної бази, розробка моделі загроз або політики безпеки для умовного підприємства). 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 з усіх чотирьох модулів курсу. 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 ІКС» 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. — 380 с.
2. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: підручник. — Житомир : ЖНАЕУ, 2023. — 636 с.
3. Луцький М. Г., Хорошко В. О., Хохлачова Ю. Є., Козловський В. В. Новітні технології захисту інформації: підручник. — Київ : НАУ, 2023. — 312 с.
4. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки: навч. посіб. — Київ : НАУ, 2022. — 298 с.
5. Євсєєв С. П., Мілов О. В., Остапов С. Е., Сєвєрінов О. В. Кібербезпека: основи кодування та криптографії: навч. посіб. — Харків : Новий Світ-2000, 2023. — 657 с.
6. Дудикевич В. Б., Хорошко В. О. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
7. Браіловський М. М., Зибін С. В., Кобозева А. А., Хорошко В. О., Хохлачова Ю. Є. Аналіз кіберзахищеності інформаційних систем: навч. посіб. — Київ : НАУ, 2023. — 276 с.
8. Корченко О. Г., Гнатюк С. О., Казмірчук С. В., Панченко В. М., Мельник С. В. Аудит та управління інцидентами інформаційної безпеки: підручник. — Київ : НАУ, 2022. — 344 с.
9. Петров В. В., Смерницький Д. В. Правові основи захисту інформації з обмеженим доступом: навч. посіб. — Харків : ХНУРЕ, 2023. — 224 с.
10. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник. — Київ : ДУІКТ, 2022. — 476 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. Офіційний сайт Верховної Ради України. — URL: **https://zakon.rada.gov.ua/**
4. Офіційний сайт Кабінету Міністрів України. — URL: **https://www.kmu.gov.ua/**
5. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
6. Міністерство цифрової трансформації України. — URL: **https://thedigital.gov.ua/**
7. Журнал «Захист інформації» (електронне видання). — URL: **https://захист-інформації.укр/**
8. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**

Рекомендована література охоплює видання **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення ОП «Організація захисту інформації в ІКС».