Силабус дисципліни «Інформаційна безпека держави»

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 безпека держави

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 безпека держави» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері забезпечення інформаційної безпеки на державному рівні. Курс спрямований на опанування концептуальних засад державної інформаційної безпеки, нормативно-правової бази, механізмів захисту інформаційного суверенітету, критичної інформаційної інфраструктури, а також сучасних загроз і методів протидії їм в умовах глобального інформаційного простору.

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 нормативно-правової та технічної інформації у сфері державної інформаційної безпеки: виявлення суттєвих загроз, порівняння механізмів захисту, формування обґрунтованих висновків щодо забезпечення інформаційної безпеки держави. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки аналітичних матеріалів, оцінки ризиків та стратегій захисту.

Здатність до усної та письмової фахової комунікації: чітко пояснювати вимоги нормативних документів у сфері державної інформаційної безпеки, аргументовано обґрунтовувати рішення щодо захисту інформаційного простору держави. Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді.

- Аналізувати нормативно-правові акти у сфері інформаційної безпеки держави
- 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 забезпечення інформаційної безпеки держави, її місця у системі національної безпеки та захисту критичної інформаційної інфраструктури. Знання ключових понять, нормативних вимог і механізмів державної системи захисту інформації, вміння застосовувати їх у практичній діяльності фахівця з комп'ютерної інженерії.

Здатність застосовувати методи забезпечення інформаційної безпеки держави для протидії сучасним кіберзагрозам, інформаційним операціям та несанкціонованому доступу до державних інформаційних ресурсів.

- Характеризувати нормативно-правову базу державної інформаційної безпеки
- Аналізувати загрози інформаційній безпеці держави та методи протидії
- Оцінювати стан захищеності критичної інформаційної інфраструктури
- Застосовувати механізми державного управління у сфері ІБ
- Здійснювати моніторинг інформаційного простору держави

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять інформаційної безпеки держави: інформаційний суверенітет, інформаційна безпека, кібербезпека, критична інформаційна інфраструктура, інформаційні загрози, інформаційно-психологічні операції. Характеризувати нормативно-правову базу, що регламентує забезпечення інформаційної безпеки України, стратегічні документи та міжнародні стандарти.

2

Аналіз та оцінювання

Аналізувати загрози інформаційній безпеці держави з точки зору джерел, характеру та наслідків впливу, виявляти вразливості державних інформаційних ресурсів та критичної інфраструктури. Оцінювати відповідність системи забезпечення інформаційної безпеки держави вимогам чинного законодавства та стратегічних документів.

3

Застосування знань

Застосовувати методи та засоби захисту державних інформаційних ресурсів, здійснювати оцінку ризиків для критичної інформаційної інфраструктури, розробляти рекомендації щодо підвищення рівня інформаційної безпеки держави в умовах гібридних та кіберзагроз.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо стану та перспектив розвитку системи інформаційної безпеки держави. Формувати професійну відповідальність і розуміння важливості захисту інформаційного суверенітету України у фаховій діяльності.

Модуль 1. Концептуальні та правові основи інформаційної безпеки держави

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Поняття та сутність інформаційної безпеки держави. Місце інформаційної безпеки в системі національної безпеки України. Основні терміни та визначення: інформаційна безпека, інформаційний суверенітет, інформаційний простір, кібербезпека. Об'єкти та суб'єкти забезпечення інформаційної безпеки держави. Принципи державної інформаційної безпеки.

Тема 1.2

Нормативно-правова база інформаційної безпеки держави. Конституція України. Закони України «Про інформацію», «Про державну таємницю», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України». Стратегія національної безпеки. Стратегія кібербезпеки України. Міжнародні стандарти ISO/IEC серії 27000.

Тема 1.3

Державна система забезпечення інформаційної безпеки. Структура та функції органів державного управління у сфері інформаційної безпеки. Роль РНБО, Держспецзв'язку, СБУ, ДКІБ. Розподіл повноважень між суб'єктами державної системи інформаційної безпеки. Міжвідомча координація та міжнародне співробітництво.

Тема 1.4

Національні інтереси та загрози в інформаційній сфері. Визначення національних інтересів України в інформаційній сфері. Класифікація загроз інформаційній безпеці держави. Зовнішні та внутрішні загрози. Актуальні загрози в умовах збройного конфлікту та гібридної війни. Індикатори та показники стану інформаційної безпеки держави.

Модуль 2. Захист критичної інформаційної інфраструктури держави

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Критична інформаційна інфраструктура (КІІ) держави. Поняття, структура та класифікація об'єктів критичної інформаційної інфраструктури. Нормативно-правове регулювання захисту КІІ в Україні. Категоризація об'єктів КІІ. Порядок визначення та ведення переліку об'єктів КІІ. Міжнародний досвід захисту КІІ.

Тема 2.2

Кіберзагрози державним інформаційним ресурсам. Класифікація кіберзагроз та кібератак на державні інформаційні системи. APT-угруповання та державні актори кіберзагроз. Аналіз реальних кіберінцидентів проти України. Методи виявлення та нейтралізації кіберзагроз. Реагування на кіберінциденти на національному рівні.

Тема 2.3

Захист державних інформаційних ресурсів та систем. Вимоги до захисту державних інформаційних ресурсів. Комплексні системи захисту інформації (КСЗІ) в державних органах. Стандарти та нормативи захисту інформації в ІКС державного призначення. Атестація та сертифікація засобів захисту інформації. Державний контроль у сфері захисту інформації.

Модуль 3. Інформаційно-психологічна безпека та протидія інформаційним операціям

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Інформаційно-психологічна безпека держави. Поняття інформаційно-психологічної безпеки. Інформаційний вплив та маніпулювання суспільною свідомістю. Дезінформація, фейки, пропаганда як інструменти інформаційних операцій. Вплив на громадську думку в цифровому середовищі. Захист суспільства від деструктивного інформаційного впливу.

Тема 3.2

Інформаційні операції та протидія їм. Поняття та класифікація інформаційних операцій. Методи проведення спеціальних інформаційних операцій. Роль ЗМІ та соціальних мереж в інформаційних операціях. Стратегічні комунікації як інструмент протидії. Система моніторингу та реагування на інформаційні загрози в Україні.

Тема 3.3

Медіабезпека та інформаційна стійкість суспільства. Роль медіапростору в системі інформаційної безпеки держави. Державна інформаційна політика та стратегічні комунікації. Медіаграмотність як складова інформаційної безпеки. Регулювання медіапростору в умовах воєнного стану. Міжнародна співпраця у сфері протидії дезінформації.

Модуль 4. Кібербезпека держави та міжнародний контекст

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Система кібербезпеки України. Структура національної системи кібербезпеки. Функції CERT-UA, Держспецзв'язку, кіберпідрозділів СБУ та інших суб'єктів. Стратегія кібербезпеки України та плани її реалізації. Реагування на кіберінциденти національного масштабу. Кіберзахист у воєнний час: досвід України.

Тема 4.2

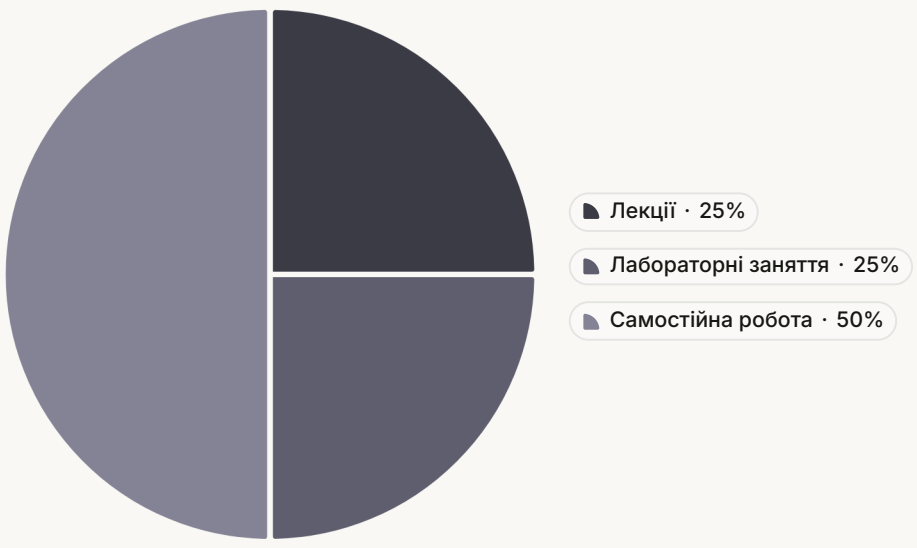
Міжнародне співробітництво у сфері інформаційної безпеки. Міжнародно-правові механізми регулювання інформаційної безпеки. Співробітництво з НАТО у сфері кіберзахисту. Конвенція Ради Європи про кіберзлочинність. Участь України в міжнародних ініціативах з інформаційної безпеки. Гармонізація законодавства України з вимогами ЄС (NIS2 Directive).

Тема 4.3

Перспективи розвитку державної інформаційної безпеки. Тенденції розвитку загроз у глобальному інформаційному просторі. Штучний інтелект як інструмент кіберзахисту та кіберзагрози. Квантові обчислення та їх вплив на інформаційну безпеку держави. Цифрова трансформація державного управління та виклики ІБ. Стратегічне планування розвитку системи інформаційної безпеки.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Поняття та сутність інформаційної безпеки держави	2	2	4
	Тема 1.2 — Нормативно-правова база	2	2	4
	Тема 1.3 — Державна система забезпечення ІБ	2	2	4
	Тема 1.4 — Національні інтереси та загрози в інформаційній сфері	2	2	4
Модуль 2	Тема 2.1 — Критична інформаційна інфраструктура	2	2	4
	Тема 2.2 — Кіберзагрози державним інформаційним ресурсам	2	2	4
	Тема 2.3 — Захист державних інформаційних ресурсів	4	4	6
Модуль 3	Тема 3.1 — Інформаційно-психологічна безпека держави	2	4	6
	Тема 3.2 — Інформаційні операції та протидія	4	4	8
	Тема 3.3 — Медіабезпека та інформаційна стійкість	2	2	6
Модуль 4	Тема 4.1 — Система кібербезпеки України	2	2	6
	Тема 4.2 — Міжнародне співробітництво у сфері ІБ	2	2	8
	Тема 4.3 — Перспективи розвитку державної ІБ	2	2	6
Разом		**30**	**30**	**60**



Структура навчального часу

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

- **Лекції (30 год. — 25%):** подача ключового теоретичного матеріалу з основ державної інформаційної безпеки
- **Лабораторні (30 год. — 25%):** практичне відпрацювання навичок аналізу загроз, дослідження КІІ, виконання захисних заходів
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, підготовка завдань, аналіз нормативних документів

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з інформаційної безпеки держави, стратегічними документами, нормативно-правовими актами, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до забезпечення державної інформаційної безпеки.

Індивідуальні завдання

Виконання аналітичних завдань щодо оцінки поточного стану інформаційної безпеки держави, аналізу конкретних кіберінцидентів, підготовка аналітичних записок з актуальних питань захисту критичної інфраструктури та протидії інформаційним операціям.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), CERT-UA (**cert.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**). Аналіз стратегічних документів, нормативних актів, звітів про кіберінциденти, методичних рекомендацій у сфері інформаційної безпеки.

Підготовка до занять

Підготовка до лабораторних занять шляхом опрацювання нормативних документів та теоретичного матеріалу; підготовка до тестувань через вивчення ключових термінів та визначень; систематизація знань перед контрольними роботами та модульними перевірками.

Методи викладання

→ Лекції

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

→ Кейс-стаді

Аналіз реальних кіберінцидентів та інформаційних операцій проти України; студенти виявляють проблему, досліджують вектори атаки, пропонують рішення та обґрунтовують висновки.

→ Лабораторні роботи

Практичне дослідження методів захисту державних інформаційних систем, аналіз інструментів виявлення загроз, оцінка захищеності об'єктів критичної інфраструктури, моделювання сценаріїв інформаційних атак.

→ Робота з нормативними документами

Опрацювання законів, стратегій, стандартів та підзаконних актів у сфері державної інформаційної безпеки; формування навичок аналізу нормативно-правового середовища.

→ Самостійне дослідження

Підготовка аналітичних записок, рефератів і презентацій за обраною темою; розвиток навичок самостійного пошуку та систематизації наукової інформації у сфері державної ІБ.

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, розбір нормативних актів та участь у вирішенні кейсів щодо реальних загроз інформаційній безпеці держави.

2

Проміжний контроль

Самостійна робота — комплексне практичне завдання або реферат, які охоплюють теми змістовних модулів (теоретичні питання, аналіз нормативної бази, оцінка загроз, розробка рекомендацій щодо захисту). 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., Толюпа С. В., Складанний П. М. Інформаційна безпека та кібербезпека держави: навч. посіб. — Київ : Видавництво «Право», 2024. — 318 с.
2. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: підручник. — Житомир : ЖНАЕУ, 2023. — 636 с.
3. Дудикевич В. Б., Хорошко В. О. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
4. Корченко О. Г., Архипов О. Є. Системи захисту інформації: стандарти та нормативна база: підручник. — Київ : НАУ, 2022. — 398 с.
5. Ліпкан В. А., Діордіца І. В. Державна політика у сфері кібербезпеки України: монографія. — Київ : ФОП Ліпкан О. С., 2023. — 276 с.
6. Петров В. В., Смерницький Д. В. Правові основи захисту інформації з обмеженим доступом: навч. посіб. — Харків : ХНУРЕ, 2023. — 224 с.
7. Складанний П. М., Гуменюк О. І., Шевченко С. М. Кібербезпека України: виклики та відповіді в умовах гібридної війни: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2023. — 256 с.
8. Толюпа С. В., Лукова-Чуйко Н. В., Шестак Я. В. Загрози та методи захисту в інформаційно-комунікаційних системах: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 292 с.
9. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник. — Київ : ДУІКТ, 2022. — 476 с.
10. Юдін О. К., Бучик С. С., Матвійчук-Юдіна О. В. Інформаційна безпека держави та критична інфраструктура: навч. посіб. — Київ : НАУ, 2024. — 340 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. Команда реагування на комп'ютерні надзвичайні події України (CERT-UA). — URL: **https://cert.gov.ua/**
3. Офіційний сайт Верховної Ради України. — URL: **https://zakon.rada.gov.ua/**
4. Рада національної безпеки і оборони України. — URL: **https://www.rnbo.gov.ua/**
5. Міністерство цифрової трансформації України. — URL: **https://thedigital.gov.ua/**
6. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
7. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**
8. Журнал «Захист інформації» (електронне видання). — URL: **https://захист-інформації.укр/**

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