МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КІБЕРБЕЗПЕКА КРИТИЧНИХ ІНФРАСТРУКТУР

методичні вказівки до практичних занять
для здобувачів першого (бакалаврського) рівня вищої освіти
галузі знань F (12) Інформаційні технології
денної та заочної форм навчання

Луцьк 2025

УДК 004.056(07)
К38
Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № від « » 20 року.

Голова вченої ради факультету КІТ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № від « » 20 року.

Завідувач кафедри КІБ Тарас ТЕРЛЕЦЬКИЙ

Укладачі: Катерина БОРТНИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: Сергій КОСТЮЧКО, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Відповідальний за випуск: Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

К38 Кібербезпека критичних інфраструктур: методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заочної форм навчання / уклад. К. Я. Бортник. Луцьк: ЛНТУ, 2025. 28 с.

Методичне видання до практичних занять з дисципліни «Кібербезпека критичних інфраструктур» складено відповідно до діючої програми курсу.

Призначене для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F (12) Інформаційні технології.

ЗМІСТ

ПРАКТИЧНЕ ЗАНЯТТЯ №1

Тема: Основи національної безпеки держави. Види національної безпеки.

Мета: Вивчення основних понять та основних категорій інформаційної безпеки.

Література: [1, 2, 5, 11, 12]

Основні задачі:

1. Вивчення основних категорій теорії національної безпеки.
2. Проведення класифікації загроз національній безпеці держави.
3. Визначення факторів та засобів забезпечення національної безпеки.
4. Класифікація базових рівнів національної безпеки.
5. Основні види національної безпеки.
6. Система забезпечення національної безпеки.
7. Розвиток ІТ-сфери в Україні.

Питання до розгляду.

1. Основні поняття та категорії теорії національної безпеки

При вивченні даного питання розглядаються базові поняття і визначення теорії національної безпеки. Вводиться поняття концепції національної безпеки. Виділяються базові національні інтереси держави. Виділяються об'єкти та принципи забезпечення національної безпеки.

2. Концепція національної безпеки України

Концепція національної безпеки України направлена на: єдність принципів формування і проведення державної політики національної безпеки; поєднання підходів до формування відповідної законодавчої бази, підготовки доктрин, стратегій, концепцій, державних і відомчих програм у різних сферах національної безпеки.

3. Загрози національній безпеці держави Класифікації загроз безпеці держави (зовнішні та внутрішні).

Загрози національній безпеці держави у різних сферах її життєдіяльності: політичній, економічній, соціальній, військовій, екологічній, науково-технічній та інформаційній.

4. Фактори та засоби забезпечення національної безпеки

Визнаються фактори забезпечення національної безпеки в економічній, соціально-політичній, духовній, воєнній, соціальній та інших сферах. Виділення факторів утвердження національної безпеки.

5. Основні рівні та види національної безпеки

Характеристика основних рівнів національної безпеки: безпека особистості, суспільства та держави. Види національної безпеки: політична, соціальна, екологічна, економічна, воєнна, науково-технічна та інформаційна безпеки. Виділення завдань забезпечення безпеки в інформаційній сфері.

6. Система забезпечення національної безпеки

Визначення системи забезпечення національної безпеки, як організованої державою сукупністю об'єктів щодо захисту національних інтересів. Функції системи забезпечення. Повноваження суб'єктів забезпечення національної безпеки.

7. Розвиток ІТ-сфера в Україні

ІТ-сектор України — один із найдинамічніших секторів української економіки. Українські ІТ-спеціалісти конкурентні на глобальному ринку, завдяки високому рівню освіти, знанню англійської, знанню актуальних технологій. Сучасний розвиток технологій привносить нові можливості в сферу кібербезпеки критичної інфраструктури. Інновації в цій галузі, такі як блокчейн, квантові технології та хмарні сервіси, дозволяють підвищити ефективність захисту даних і систем управління, а також забезпечити більшу стійкість до атак.

Питання для самоконтролю:

1. Що таке національна безпека?
2. Назвіть основні категорії теорії національної безпеки.
3. Основна ідея концепції національної безпеки.
4. Назвіть базові рівні національної безпеки.
5. Охарактеризуйте основні види національної безпеки України.
6. Назвіть новітні технології захисту даних.

ПРАКТИЧНЕ ЗАНЯТТЯ №2

Тема: Організаційна модель кібербезпеки для об’єкта критичної інфраструктури.

Мета: Показати, як організована структура захисту об’єктів критичної інфраструктури.

Література: [1, 2, 5, 6, 10]

Основні задачі:

1. Рівень стратегічного управління.
2. Рівень тактичного управління.
3. Рівень операційної безпеки.
4. Рівень експлуатації інфраструктури.
5. Контроль та зовнішня взаємодія.

Питання до розгляду.

1. Рівень стратегічного управління

Це верхній рівень, який визначає політику, ресурси та пріоритети. Керівник об’єкта критичної інфраструктури формує політику кібербезпеки, затверджує фінансування та план захисту, несе відповідальність за відповідність законодавству.

2. Рівень тактичного управління

Реалізація політики підприємства, керування безпековими підрозділами, оцінка кіберризиків, перевірка відповідності стандартам та законам.

3. Рівень операційної безпеки

На цьому рівні здійснюються реальні технічні заходи захисту й реагування. Це: моніторинг; виявлення та аналіз атак; аналіз трафіку; реагування на інциденти; взаємодія з національним CERT-UA; оцінка ризиків для промислових систем; управління фаєрволами, VPN, сегментацією мереж; контроль доступу, управління обліковими записами.

4. Рівень експлуатації інфраструктури

Тут знаходяться підрозділи, які працюють безпосередньо з IT і виробничими системами. Вони відповідають за підтримку серверів, мереж, робочих станцій; дотримання вимог кібербезпеки; відповідають за стабільну роботу SCADA, DCS, PLC, каналів передачі даних.

5. Контроль та зовнішня взаємодія

Обов’язкова координація з державою та зовнішніми структурами. Об’єкти критичної інфраструктури зобов’язані проходити внутрішній аудит кібербезпеки, зовнішній сертифікаційний аудит, постійно взаємодіяти з Національним координаційним центром кібербезпеки (НКЦК), з галузевими центрами.

Питання для самоконтролю:

1. Що таке політика кібербезпеки?
2. Які функції виконує Національний координаційний центр кібербезпеки.
3. Повноваження головного спеціаліста з інформаційної безпеки.
4. Які задачі вирішуються на рівні операційної безпеки.
5. Назвати відповідальних за виконання задач на рівні експлуатації інфраструктури.
6. Навести приклади порушення безпеки.

ПРАКТИЧНЕ ЗАНЯТТЯ №3

Тема: Освітні домени в галузі Кібербезпеки. Моделі загроз в сучасному кіберпросторі.

Мета: Ознайомити з можливими моделями загроз в кіберпросторі.

Література: [1, 2, 5]

Основні задачі:

1. Класифікація освітніх доменів в галузі Кібербезпеки.
2. Кіберпростір.
3. Моделі загроз в кіберпросторі.

Питання до розгляду.

1. Домени Кібербезпеки.

Визначення поняття домену. Розглядаємо, характеризуємо освітні домени в галузі Кібербезпеки: фундаментальні основи інформаційної безпеки; криптографія та захист даних; мережна безпека; операційні системи та їх безпека; безпека прикладного програмного забезпечення; кіберзахист критичної інфраструктури; управління інцидентами; управління ризиками, аудит та комплаєнс; хмарна безпека; тестування безпеки; соціальна інженерія та поведінкова безпека; правові та етичні аспекти кібербезпеки.

2. Кіберпростір. Моделі загроз в сучасному кіберпросторі

Що собою являє кіберпростір. Аналіз моделей загроз, які використовують для аналізу ризиків, побудови захисту та проєктування безпечних систем.

STRIDE (Microsoft) – одна з найпоширеніших моделей, використовується для аналізу загроз на етапі проєктування систем. Добре працює для вебсервісів, додатків, архітектурних рішень.

DREAD – модель для кількісної оцінки серйозності загрози. Вона працює за такими показниками, як: потенційна шкода (D); повторюваність атаки (R); складність експлуатації (E); кількість постраждалих користувачів (A); ймовірність виявлення вразливості (D).

MITRE ATT&CK – глобальна база знань про тактики та техніки зловмисників.

Cyber Kill Chain – модель, яка описує фази кібернападу. Використовується для SOC, тестування й захисту критичної інфраструктури. Етапи цієї моделі наступні: розвідка, створення шкідливого інструменту, доставка, експлуатація вразливості, закріплення в системі, встановлення зв’язку, крадіжка, руйнування, саботаж.

PASTA – 7-етапна модель, орієнтована на бізнес-ризики. Використовується великими компаніями й у сфері критичної інфраструктури. Дана модель враховує бізнес-процеси, фінансовий вплив, контекст організації, моделює атаки з погляду впливу на бізнес, аналізує ймовірність та наслідки.

LINDDUN – модель орієнтована на аналіз конфіденційності та персональних даних.

OWASP – модель загроз для додатків.

Питання для самоконтролю:

1. Що таке кіберпростір?
2. Назвіть основні моделі загроз для об’єкта критичної інфраструктури.
3. Охарактеризуйте модель загроз Cyber Kill Chain.
4. Яка мета моделей загроз?
5. Навести приклади доменів в галузі Кібербезпеки.

ПРАКТИЧНЕ ЗАНЯТТЯ №4

Тема: Аналіз кібератаки. Типи зловмисного програмного забезпечення.
Мета: Вивчення основних типів зловмисного ПЗ.
Література: [1, 2, 3, 5]

Основні задачі:
1. Що таке кібервійна.
2. Наслідки кібератак.
2. Види та типи зловмисного програмного забезпечення.
3. Антивірусне програмне забезпечення.
4. Заходи профілактики.

Питання до розгляду.

1. Наслідки кібератак

Наслідки кібератак у різних сферах життєдіяльності країни: політичній, економічній, соціальній, військовій, екологічній, науково-технічній та інформаційній.

2. Основні види шкідливого ПЗ

Характеристика основних видів шкідливого програмного забезпечення, етапи поширення.

3. Антивірусне програмне забезпечення.

Спеціальне ативірусне програмне забезпечення для боротьби з вірусами. Види антивірусів. Методи антивірусного захисту.

4. Заходи профілактики

Регулярне виконання антивірусних програм, одночасне обстеження всієї системи на віруси.

Питання для самоконтролю:

1. Назвати симптоми шкідливого програмного забезпечення.
2. Визначити типи шкідливих програм:

− шкідливе програмне забезпечення, призначене для автоматичного виконання дій, здебільшого в інтернеті?;

− шкідливе програмне забезпечення, призначене для блокування комп'ютерної системи або даних до моменту отримання викупу?;

− шкідливе програмне забезпечення, призначене для виконання змін у операційній системі з метою створення чорного ходу?;

− шкідливе програмне забезпечення, яке часто розповсюджується в комплекті з легальним та призначене для відстежування активності користувача?;

− шкідливий виконуваний код, який додається до інших виконуваних файлів, часто легальних програм?;

− зловмисне програмне забезпечення, яке здійснює шкідливі дії під виглядом бажаної операції?;

− шкідлива програма, яка призначена для автоматичного поширення реклами. Інколи розповсюджується в комплекті з іншим програмним забезпеченням?;

− зловмисне програмне забезпечення, яке використовується для захоплення контролю над мобільним пристроєм?;

− шкідливе програмне забезпечення, яке переконує користувача здійснити конкретну дію, використовуючи його страх?;

− шкідливий код, який самостійно клонує себе, використовуючи вразливості в мережах?.

ПРАКТИЧНЕ ЗАНЯТТЯ №5

Тема: Потреба в кібербезпеці. Тріада CIA.

Мета: Донести основні принципи кібербезпеки.

Література: [1, 2, 3, 5]

Основні задачі:

1. Захист персональних даних.
2. Дані організації.
3. Конфіденційність, цілісність та доступність.

Питання до розгляду.

1. Що таке кібербезпека?

При вивченні даного питання пояснюється, що таке кібербезпека і чому зростає попит на фахівців з кібербезпеки. Пояснюється, що таке онлайн-ідентифікація та що таке дані, де вони знаходяться і чому це цікавить кібер-злочинців.

2. Захист персональних даних

Ваша онлайн та офлайн ідентифікація, ваші дані, де знаходяться ваші дані?, ваші комп'ютерні пристрої, злочинцям потрібна ваша особистість.

3. Дані організації

Розглядаються типи даних організації: традиційні дані - корпоративні дані, які включають інформацію про персонал, інтелектуальну власність та фінансові дані; Інтернет речей (Internet of Things, IoT) та великі дані (BigData).

4. Конфіденційність, цілісність та доступність

Конфіденційність, цілісність та доступність, відома як тріада CIA, є керівним принципом для безпеки інформації для організації. Конфіденційність гарантує конфіденційність даних, обмежуючи доступ до них через механізм аутентифікації. Цілісність гарантує точність і достовірність інформації. Доступність гарантує, що інформація доступна для авторизованих користувачів.

Питання для самоконтролю:

1. Що таке кібербезпека?
2. Назвіть основні задачі кібербезпеки.
3. Основні засади конфіденційності.
4. Основні засади цілісності.
5. Основні засади доступності.
6. Навести приклади порушення безпеки.

ПРАКТИЧНЕ ЗАНЯТТЯ №6

Тема: Складові кібербезпеки для об’єктів критичної інфраструктури. Хмарні інфраструктурні сервіси.

Мета: Як правильно організувати кіберзахист критичних інфраструктур.

Література: [1, 2, 5, 6]

Основні задачі:

1. Контроль доступу та ідентифікація.
2. Навчання персоналу.
3. Управління ризиками.
4. Моніторинг і виявлення інцидентів.
5. Реагування на інциденти та відновлення.
6. Захист мережевої інфраструктури.
7. Фізична безпека.
8. Хмарні інфраструктурні сервіси.

Питання до розгляду.

1. Контроль доступу та ідентифікація

Мінімізація прав, багатофакторна автентифікація, контроль привілейованих облікових записів.

2. Навчання персоналу

Сертифікація фахівців, постійне підвищення рівня оперативного персоналу, підвищення культури безпеки.

3. Управління ризиками

Типи ризиків. Оцінювання загроз для IT та OT-систем, визначення критичних активів і застосування заходів для зниження ризиків.

4. Моніторинг і виявлення інцидентів

Аналіз телеметрії, виявлення аномалій у реальному часі.

5. Реагування на інциденти та відновлення

NIST, життєвий цикл реагування на інцидент. Дії після інциденту. Збір та збереження даних про інциденти. Вимоги до звітування та поширення інформації.

6. Захист мережевої інфраструктури

Сегментація мережі, фаєрволи, IDS/IPS, захист каналів зв’язку, розмежування IT та OT-сектора.

7. Фізична безпека

Контроль доступу до об'єктів, відеоспостереження, захист обладнання від фізичного втручання.

8. Хмарні інфраструктурні сервіси

Хмарні служби зберігання та резервного копіювання. Хмарні рішення з безпеки. Надання віртуалізованих ресурсів.

Питання для самоконтролю:

1. Як працює багатофакторна автентифікація.
2. Назвіть типи ризиків.
3. Назвіть етапи життєвого циклу реагування на інцидент.

4. Елементом якої частини плану реагування на інцидент є стратегії та цілі?

ПРАКТИЧНЕ ЗАНЯТТЯ №7

Тема: Політики та процедури кібербезпеки. Методи проникнення.

Мета: Знати, що таке політики та процедури кібербезпеки та ознайомлення з основними методами проникнення до даних.

Література: [1, 2, 3, 5]

Основні задачі:

1. Поняття політики кібербезпеки.
2. Поняття процедури кібербезпеки.
3. Атаки на автентифікацію та облікові дані.
4. Експлуатація вразливостей програмного забезпечення.
5. Соціальна інженерія.
6. Внутрішні порушники.

Питання до розгляду.

1. Поняття політики кібербезпеки

Політика кібербезпеки – це стратегічний документ, що встановлює загальні принципи, вимоги та підходи до захисту інформації в організації. Тут описуються правила, конкретні вимоги, що повинен виконувати кожен на своєму місці, обов'язкові для всієї організації; Також забезпечує узгодженість і стандартизацію підходів та слугує основою для розробки детальних процедур.

2. Поняття процедури кібербезпеки

Процедури – це детальні, покрокові інструкції, що описують, як саме виконувати конкретні дії для забезпечення безпеки. Наприклад, процедура реагування на кіберінцидент; процедура створення та зберігання резервних копій; процедура надання та відкликання доступу користувачам. Тобто, будь яка дія щодо захисту інформації має конкретну покрокову інструкція, яка підлягає точному виконанню.

В цілому, політики та процедури кібербезпеки – це основні нормативні документи, які визначають правила, стандарти та порядок дій для захисту інформаційних ресурсів організації. Вони формують основу системи управління безпекою та забезпечують узгодженість дій персоналу.

3. Атаки на автентифікацію та облікові дані

Фішинг. Обман користувача через підроблені листи, сайти чи повідомлення з метою отримання логінів, паролів, токенів. Цілеспрямовані атаки на конкретних працівників або керівництво, що відкривають доступ до корпоративних систем. Перебір комбінацій паролів або використання найпоширеніших.

4. Експлуатація вразливостей програмного забезпечення

Вразливості програмного забезпечення, як правило, є наслідками помилок в коді операційної системі або програми. Також, зловмисники можуть впроваджувати шкідливий SQL-код через форму.

5. Соціальна інженерія

Найбільш поширений метод, в основі якого лежить створення довірчої ситуації, дзвінки або SMS із метою отримання доступу до систем чи даних,

листи із запропонованими принадами.

6. Внутрішні порушники

Це співробітник, який свідомо викрадає чи продає дані або ненавмисні помилки.

Питання для самоконтролю:

1. Яка відмінність між процедурами та стандартами?
2. Яка мета політики кібербезпеки.
3. Роль процедур кібербезпеки. Наведіть приклади.
4. Охарактеризуйте метод проникнення «Соціальна інженерія».
5. Наведіть приклад вразливостей апаратного забезпечення.

ПРАКТИЧНЕ ЗАНЯТТЯ №8

Тема: Стратегії контролю доступу. Забезпечення цілісності баз даних.

Мета: Ознайомлення з різними моделями надання доступу, як забезпечити цілісність баз даних.

Література: [1, 2, 4, 5]

Основні задачі:

1. Мандатний контроль доступу (MAC).
2. Дискреційний контроль доступу (DAC).
3. Рольовий контроль доступу (RBAC).
4. Атрибутивний контроль доступу (ABAC).
5. Нульова довіра (ZTA).
6. Логічні механізми цілісності на рівні СУБД.
7. Технічні та архітектурні механізми.
8. Захист від несанкціонованих змін.
9. Захист інфраструктури.
10. Організаційні заходи.

Питання до розгляду.

1. Мандатний контроль доступу

Стратегії контролю доступу – це моделі та підходи, які визначають, хто, як і за якими правилами може отримувати доступ до інформаційних ресурсів. Вони забезпечують захист даних, мінімізують ризики несанкціонованого доступу та формують основу кібербезпеки організації.

Доступ визначається централізованою політикою, а не власником ресурсу. Користувачі та дані мають рівні секретності. Дана модель має найвищий степінь захисту.

2. Дискреційний контроль доступу

Доступ визначається власником ресурсу.

3. Рольовий контроль доступу

Доступ ґрунтується на ролях, а ролі пов'язані з посадовими обов’язками.

4. Атрибутивний контроль доступу

Доступ визначається набором атрибутів, а не ролями чи рівнями.

5. Нульова довіра

Модель, де нікому не довіряють за замовчуванням. За таких умов, відбувається постійна перевірка користувача і пристрою, мінімальні привілеї.

6. Логічні механізми цілісності на рівні СУБД

До логічних механізмів відносимо вбудовані правила, що не дозволяють записувати некоректні дані; автоматичні процедури, які контролюють зміни даних; принцип ACID, за яким зміни виконуються повністю або не виконуються зовсім.

7. Технічні та архітектурні механізми

До цього типу механізму відносимо журнал транзакцій, де фіксуються зміни в базах даних перед виконанням певної задачі; резервне копіювання; синхронне або асинхронне дублювання даних між серверами.

8. Захист від несанкціонованих змін

Тут розглядаємо хешування даних, цифрові підписи, контроль версій.

9. Захист інфраструктури

До цієї категорії забезпечення цілісності даних відносимо шифрування каналів, сегментація мережі, багатофакторна автентифікація до СУБД та регулярні оновлення.

10. Організаційні заходи

Процедури зміни даних, перевірки та аудит.

Питання для самоконтролю:

1. Які види обмежень використовуються в СУБД для підтримки цілісності даних? Наведи приклади.

2. Що таке реплікація даних і як вона впливає на доступність та цілісність БД?

3. Що таке цілісність бази даних і чому вона є критично важливою для організацій?

4 Поясни принцип ACID. Як кожен із його елементів впливає на цілісність даних?

5. Як журнал транзакцій (Write-Ahead Log) допомагає у відновленні бази після збоїв?

6. Наведи приклад атрибутивного контролю доступу.

7. Наведи приклади ситуацій, у яких може бути порушена цілісність даних. Які механізми запобігли б цьому?

8. Які основні види цілісності даних ти знаєш?

9. Як контроль доступу може впливати на цілісність бази даних?

ПРАКТИЧНЕ ЗАНЯТТЯ №9

Тема: Реагування на інциденти. Захист бездротових та мобільних пристроїв. Захист систем та пристроїв.

Мета: Ознайомлення з послідовністю дій при реагуванні на інциденти, як захиститись від вторгнень на апаратному рівні.

Література: [1, 2, 3, 5]

Основні задачі:

1. Підготовка.
2. Виявлення та ідентифікація інциденту.
3. Стримування.
4. Усунення.
5. Відновлення.
6. Технології захисту бездротових та мобільних пристроїв.

Питання до розгляду.

1. Підготовка

Розглядаємо задачі формування команди реагування, створення політик і процедур реагування, встановлення систем моніторингу, навчання персоналу, наявність контактів та інструментів для реагування.

2. Виявлення та ідентифікація інциденту

Розглядаємо, яким чином з'ясувати, що інцидент відбувся, класифікувати тип інциденту, оцінити масштаб і критичність та встановити пріоритет реагування,

3. Стримування

Вивчаємо, як зупинити розповсюдження інциденту та обмежити шкоду.

4. Усунення

Розглядаємо, яким чином повністю видалити наслідки інциденту та джерело компрометації.

5. Відновлення

Вивчаємо, яким чином повернути системи до нормальної роботи без ризику повторного інциденту.

6. Технології захисту бездротових та мобільних пристроїв

Розглядаємо такі технології, як шифрування, аутентифікація користувачів, поділ мережі на окремі VLAN, фільтрація MAC-адрес, контейнеризація корпоративних даних, контроль доступу до корпоративних ресурсів через Zero Trust.

Питання для самоконтролю:

1. Які перші кроки потрібно зробити, коли стався якійсь інцидент?
2. Назвіть типи інцидентів?
3. У чому суть підходу Zero Trust щодо мобільних та бездротових пристроїв?
4. Чому сегментація мережі (VLAN) важлива у бездротових інфраструктурах?
5. Які ризики пов'язані з Bluetooth та як їх можна мінімізувати?

6. У чому полягає перевага контейнеризації даних на мобільному пристрої?

ПРАКТИЧНЕ ЗАНЯТТЯ №10

Тема: Європейський досвід забезпечення кібербезпеки об’єктів критичної інфраструктури.

Мета: Ознайомлення з досвідом інших країн світу щодо захисту об’єктів критичної інфраструктури.

Література: [1, 2, 5, 6, 9, 10]

Основні задачі:

1. Законодавство.
2. Централізована технічна підтримка.
3. Інституційна модель і координація.
4. Практики і технічні підходи.

Питання до розгляду.

1. Законодавство

При вивченні даного питання розглядаємо законодавчу базу ЄС, зокрема, директиву NIS2, яка розширює сфери й обов’язки для «важливих» і «ключових» суб’єктів, вводить обов’язкові заходи ризик-менеджменту і жорсткіші вимоги до звітності та санкцій.

2. Централізована технічна підтримка

ENISA (European Union Agency for Cybersecurity) – це Агентство Європейського Союзу з кібербезпеки, головна структура ЄС, що відповідає за зміцнення кіберстійкості держав-членів, координацію дій та розвиток стандартів безпеки. Вона розробляє стандарти, проводить аналітику, організовує навчання та координує реагування на інциденти.

3. Інституційна модель і координація

Знайомимся із загальною практикою централізованої координації інцидентів, обміну розвідданими та інформування про зломи в межах ЄС.

4. Практики і технічні підходи

Кращі практики ЄС: обов’язкова звітність і оперативне реагування; ризик-орієнтовані вимоги; секторні та індустріальні стандарти.

Питання для самоконтролю:

1. Що таке ENISA і які основні завдання виконує ця агенція?
2. Яким чином ENISA підтримує сектор критичної інфраструктури?
3. Які основні типи аналітичних звітів щороку публікує ENISA?
2. У чому полягає роль ENISA у координації реагування на кіберінциденти між країнами ЄС?

ПРАКТИЧНЕ ЗАНЯТТЯ №11

Тема: Партнерство держави й приватного сектору.

Мета: Розглянути, як взаємодія держави та приватного сектору підвищує безпеку.

Література: [1, 2, 5, 9, 10]

Основні задачі:

1. Обмін розвідкою.
2. Спільні проекти та програми.
3. Успішні практики.

Питання до розгляду.

1. Обмін розвідкою

При вивченні даного питання розглядаються новітні кібератаки на різних рівнях, їх локалізація, відновлення та обмін досвідом.

2. Спільні проекти та програми

У США для пошуку вразливостей кіберзахисту на об’єктах сектору безпеки і оборони ініційовано кілька успішних державно-приватних програм та проектів. У межах перевірки стану кібербезпеки, реалізовано проект «Зламай Пентагон».

Подібною ініціативою в США є програма «Зламай Військово-повітряні сили» («Hack the Air Force»). За час програми було виявлено і усунено понад 120 вразливостей кіберзахисту Військово-повітряних сил США. Тобто, метою таких програм є тестування на проникнення та виявлення слабких місць у захисті інформаційних систем від кібератак та подальше їх усунення.

3. Успішні практики

Естонія: висока цифровізація, сильна національна архітектура кібербезпеки, постійні вправи і модель з інтегрованим реагуванням.

Питання для самоконтролю:

1. Наведіть приклади кращих практик кіберзахисту.
2. Ваша думка, щодо партнерства держави й приватного сектору в Україні.

ПРАКТИЧНЕ ЗАНЯТТЯ №12

Тема: Аудити та оцінка відповідності інформаційних систем.
Мета: Дізнатися, що таке аудит ІС, його типи та які задачі він виконує.
Література: [1, 2, 3, 5, 9]

Основні задачі:
1. Мета аудиту та оцінки відповідності.
2. Етапи проведення аудиту.

Питання до розгляду.

1. Мета аудиту та оцінки відповідності

При вивченні даного питання, розглядаємо, яка мета аудиту та якими чинниками керуються аудитори, аби оцінити наскільки ІТ-система відповідає вимогам безпеки, стандартам, політикам та законодавству.

2. Етапи проведення аудиту

Сюди відносимо: підготовка та планування; оцінка документів і політик; технічна перевірка; інтерв'ю з персоналом; аналіз відповідності та формування звіту.

Питання для самоконтролю:

1. Чим аудит відрізняється від оцінки відповідності?
2. Що таке доказова база в аудиті і як її збирають?
3. Що таке критерії аудиту та як вони визначаються?
4. Які основні методи збору доказів використовують аудитори?
5. Які міжнародні стандарти найчастіше використовують при оцінці відповідності інформаційних систем (наприклад, ISO 27001, NIST)?

ПРАКТИЧНЕ ЗАНЯТТЯ №13

Тема: Стандартизація послуг в сфері кібербезпеки.

Мета: Дізнатися, яку роль відіграє стандартизація послуг в сфері кібербезпеки в плані захисту інформаційних систем.

Література: [1, 2, 3, 5]

Основні задачі:

1. Міжнародні та національні стандарти кібербезпеки.
2. Стандарти послуг безпеки.
3. Стандартизація процесів управління кібербезпекою.
4. Стандарти для критичної інфраструктури.

Питання до розгляду.

1. Міжнародні та національні стандарти кібербезпеки

Розглядаємо ISO/IEC 27001, 27002 – управління інформаційною безпекою; ISO/IEC 27035 – управління інцидентами; ISO/IEC 27701 – захист персональних даних.

2. Стандарти послуг безпеки

Розглядаємо ISO/IEC 19011 – аудит і оцінка відповідності; CVSS, стандарти NIST – управління вразливостями.

3. Стандартизація процесів управління кібербезпекою

Розглядаємо управління ризиками, реагування на інциденти резервне копіювання та відновлення, контроль доступу.

4. Стандарти для критичної інфраструктури

Директиви ЄС та рекомендації ENISA, включно з вимогами до кіберстійкості, безперервності діяльності, захисту мережевих та промислових систем (ICS/SCADA).

Питання для самоконтролю:

1. Які стандарти використовуються для проведення тестування на проникнення?
2. Чому стандартизація є важливою для якості та надійності послуг з кібербезпеки?
3. Що визначають стандарти ENISA та директива NIS2 для критичної інфраструктури?
4. Які ключові процеси повинні бути стандартизовані в організації для забезпечення належного рівня кіберзахисту?

ПРАКТИЧНЕ ЗАНЯТТЯ №14

Тема: Сертифікація в галузі кібербезпеки.
Мета: Дізнатися, що таке сертифікація та її види.
Література: [1, 2, 5, 11, 12]

Основні задачі:
1. Сертифікація фахівців.
2. Сертифікація процесів.
3. Сертифікація продуктів та технологій.

1. Сертифікація фахівців

Розглядаємо сертифікаційні центри в Україні в галузі кібербезпеки та найвідоміші міжнародні.

2. Сертифікація процесів

Сертифікація процесів – це офіційний документ, в якому підтверджується, що організація впровадила систему управління безпекою.

3. Сертифікація продуктів та технологій

Розглядаємо, хто проводить сертифікацію продуктів та технологій в сфері кібербезпеки, для кого вона є обов'язковою.

Питання для самоконтролю:

1. Чим відрізняється персональна сертифікація від сертифікації організацій?
2. Як сертифікація сприяє підвищенню кіберстійкості критичної інфраструктури?
3. Що таке сертифікація у сфері кібербезпеки та яку мету вона виконує?
4. Які міжнародні сертифікати підтверджують компетентність кіберфахівця? Наведи приклади.

ПРАКТИЧНЕ ЗАНЯТТЯ №15

Тема: Концептуальні підходи до кадрів в кібербезпеці. Правові та нормативні засади забезпечення кібербезпеки в Україні.

Мета: Окреслити основні професійні вимоги та відповідальність в кібербезпеці.

Література: [1, 2, 5]

Основні задачі:

1. Національна концепція професійної підготовки в сфері кібербезпеки.
2. Персональні юридичні питання.
3. Корпоративні правові питання.
4. Корпоративні етичні питання.

Питання до розгляду.

1. Нестача фахівців з кібербезпеки.

Європейський досвід у запровадженні сучасних підходів у сфері безпеки, огляд форм і форматів навчальних курсів щодо підготовки кадрів, досвід організації підготовки кадрів на прикладі досвіду США, національна концепція професійної підготовки в сфері кібербезпеки, співпраця з міжнародними організаціями в цій сфері.

2. Персональні юридичні питання

Закон України «Про інформацію» (№ 2657-XII від 02.10.1992).

3. Корпоративні правові питання

Закон «Про основні засади забезпечення кібербезпеки України» (5 жовтня 2017 року).

4. Корпоративні етичні питання

Кодекс етики, контракти з працівниками ІТ та ІБ.

Пит*ання для самоконтролю:*

1. Як нестача спеціалістів впливає на захист критичних інфраструктур та забезпечення її стійкості?
2. Основні особливості формування компетентностей фахівців з кібербезпеки?
3. Яка передбачена відповідальність за несанкціонований доступ, втручання, знищення або блокування даних?
4. Для яких працівників сертифікація є обовязковою?

Список рекомендованих джерел

1. Копча В. І., Грищук Р. В. Кібербезпека критичних інформаційних інфраструктур: навч. посібник Київ, 2022.
2. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Київ : Видавництво НА СБ України, 2020. 256 с.
4. Шваюк А.В., Бортник К.Я., Гринюк С.В. Аналіз методів тестування на проникнення в ком'ютерні системи для оцінки якості захисту банківських даних користувачів // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво» – Луцьк: Видавництво ЛНТУ. Вип. 42. 2021. С. 218-222.
5. Курс мережевої академії Cisco: Cybersecurity Essentials, 2020. URL: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials (дата звернення: 10.09.2025).
6. Кібербезпека для енергетичних та промислових систем: URL: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi (дата звернення: 10.10.2025).
7. Базові знання з кібергігієни. URL: https://surl.lu/dqsfpx (дата звернення: 10.10.2025).
8. Закон України «Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.05.2025).
9. Аналіз кращих світових практик щодо захисту критичної інформаційної інфраструктури. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/218/195 (дата звернення: 12.09.2025).
10. NIST Cybersecurity Framework (CSF) 2.0 (2024) – основа кіберзахисту критичної інфраструктури США. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 15.09.2025).
11. Закон України "Про захист інформації в автоматизованих системах".
12. Про основні засади забезпечення кібербезпеки України, Закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.10.2025).

Кібербезпека критичних інфраструктур: методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заочної форм навчання / уклад. К. Я. Бортник. Луцьк: ЛНТУ, 2025. 28 с

К-38

Методичне видання до практичних занять з дисципліни «Кібербезпека критичних інфраструктур» складено відповідно до діючої програми курсу.

Призначене для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F (12) Інформаційні технології.

Комп’ютерний набір К. Я. Бортник

Редактор К. Я. Бортник

Підп. до друку «___» _____ 2025р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75