Міністерство освіти і науки України
Національний університет водного господарства та природокористування

Навчально-науковий інститут права
Кафедра інформаційного права та юридичної журналістики

08-04-25М

МЕТОДИЧНІ ВКАЗІВКИ

до організації практичних занять
та виконання самостійної роботи
з навчальної дисципліни
«**Інформаційна безпека**»
для здобувачів вищої освіти другого
(магістерського) рівня
за освітньо-професійної програми
«Медіаправо та медіабезпека»
спеціальності 061 «Журналістика»
денної та заочної форми навчання

Рекомендовано науково-
методичною
радою з якості ННІП
Протокол № 10 від 21.03.2025 р.

Рівне – 2025

Методичні вказівки до практичних занять та виконання самостійної роботи з навчальної дисципліни «Інформаційна безпека» для здобувачів вищої освіти другого (магістерського) рівня за освітньо-професійною програмою «Медіаправо та медіабезпека» спеціальності 061 «Журналістика» денної та заочної форми навчання. [Електронне видання] / Мітчук О. А. – Рівне : НУВГП, 2025. – 53 с.

Укладач:
Мітчук О. А., доктор наук із соціальних комунікацій, професор, професор кафедри інформаційного права та юридичної журналістики.

Відповідальний за випуск: Мітчук О. А., доктор наук із соціальних комунікацій, професор, в.о. завідувача кафедри інформаційного права та юридичної журналістики.

Керівник групи забезпечення
спеціальності 061 «Медіаправо та медіабезпека»
Мітчук О. А.

ЗМІСТ

ПЕРЕДМОВА

У сучасному світі, де цифрові технології проникають у кожен аспект нашого життя – від особистого спілкування до управління критичною інфраструктурою – питання інформаційної безпеки набуває першочергового значення. Це не просто набір технічних інструментів, а комплексна система знань, навичок та принципів, що забезпечують захист даних, систем та мереж від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення.

Дисципліна «Інформаційна безпека» є фундаментальною для кожного, хто прагне розуміти та ефективно протистояти зростаючій кількості загроз у кіберпросторі. Вона навчить вас розпізнавати вразливості, оцінювати ризики, застосовувати ефективні методи захисту та оперативно реагувати на інциденти. Ви опануєте не лише технічні аспекти, а й правові, організаційні та етичні засади забезпечення безпеки інформації.

Ці методичні вказівки стануть вашим надійним помічником у вивченні складного, але надзвичайно захопливого світу інформаційної безпеки. Вони допоможуть вам систематизувати знання, відпрацювати практичні навички та підготуватися до викликів, які постають перед фахівцями у цифрову епоху. У світі, де цифрові технології проникають у кожен аспект нашого життя – від особистого спілкування до управління критичною інфраструктурою – питання інформаційної безпеки набуває першочергового значення. Це не просто набір технічних інструментів, а комплексна система знань, навичок та принципів, що забезпечують захист даних, систем та мереж від несанкціонованого

доступу, використання, розкриття, порушення, модифікації або знищення.

Актуальність вивчення дисципліни «Інформаційна безпека» зумовлена низкою факторів:

Тотальна цифровізація: Сучасне суспільство повністю залежить від інформаційних технологій. Це створює величезні можливості, але й несе значні ризики, адже будь-який збій або атака на інформаційні системи може мати катастрофічні наслідки для економіки, соціальної сфери та національної безпеки.

Зростання кіберзлочинності: Кількість та складність кібератак постійно зростають. Від фішингу та вірусів-здирників до складних цільових атак на державні установи та критичну інфраструктуру – кіберзлочинність стає глобальною загрозою.

Захист персональних даних: В умовах стрімкого збору та обробки персональних даних, їх захист стає пріоритетом. Законодавство, таке як GDPR, встановлює суворі вимоги до організацій, а порушення цих норм веде до значних штрафів та втрати довіри.

Інформаційні війни та гібридні загрози: Інформація використовується як зброя у гібридних конфліктах. Розуміння механізмів поширення дезінформації, пропаганди та кібератак є критично важливим для захисту національного інформаційного простору.

Забезпечення безперервності бізнесу та функціонування держави: Надійний захист інформаційних систем є запорукою стабільної роботи підприємств, державних органів та критичної інфраструктури, що є основою стійкості суспільства.

Ці методичні вказівки стануть вашим надійним помічником у вивченні складного, але надзвичайно

захопливого світу інформаційної безпеки. Вони допоможуть вам систематизувати знання, відпрацювати практичні навички та підготуватися до викликів, які постають перед фахівцями у цифрову епоху. Ви опануєте не лише технічні аспекти, а й правові, організаційні та етичні засади забезпечення безпеки інформації.

освіти всебічної підтримки у самостійному опрацюванні теоретичного матеріалу, ретельній підготовці до практичних занять та успішному виконанні індивідуальних завдань. Особливий акцент зроблено на практико-орієнтованому навчанні, включаючи аналіз конкретних ситуацій (Case-study), що сприяє розвитку аналітичних та прикладних навичок, необхідних для застосування європейських стандартів у сфері медіаправа та медіабезпеки.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ТА ЇЇ СТРУКТУРА

1.1. Опис навчальної дисципліни

Метою викладання дисципліни «Інформаційна безпека» є формування у здобувачів вищої освіти комплексних знань, умінь та практичних навичок, необхідних для розуміння загроз інформаційній безпеці, принципів її забезпечення, а також застосування сучасних методів та засобів захисту інформації в різних сферах діяльності. Дисципліна має на меті підготувати фахівців, здатних ідентифікувати, аналізувати та ефективно протидіяти кіберзагрозам, забезпечуючи конфіденційність, цілісність та доступність інформації.

Завданнями навчальної дисципліни є:

- Ознайомлення з основними поняттями та принципами інформаційної безпеки: вивчення визначень, складових інформаційної безпеки (конфіденційність, цілісність, доступність), класифікації загроз та вразливостей.
- Вивчення нормативно-правового забезпечення інформаційної безпеки: надання знань щодо національних та міжнародних законодавчих актів, стандартів та регуляторних вимог у сфері кібербезпеки та захисту інформації.
- Аналіз методів та засобів захисту інформації: розгляд програмних, апаратних, організаційних та фізичних методів захисту інформації, криптографічних засобів, систем виявлення вторгнень.
- Навчання управління ризиками

інформаційної безпеки: формування навичок з ідентифікації, оцінки та мінімізації ризиків, розробки політик безпеки.

- Освоєння основ аудиту та моніторингу інформаційної безпеки: вивчення методів проведення аудиту безпеки, моніторингу подій та реагування на інциденти.
- Розвиток практичних навичок з використання засобів захисту: робота з антивірусним програмним забезпеченням, фаєрволами, системами резервного копіювання тощо.
- Набуття знань про особливості захисту інформації в різних інформаційних системах (корпоративні мережі, веб-ресурси, хмарні технології, мобільні пристрої).
- Розгляд питань кіберзлочинності та кібервійни: ознайомлення з основними видами кіберзлочинів, методами їх розслідування та протидії.

Вивчення освітньої компоненти супроводжується набуттям таких компетентностей та результатів навчання:

Інтегральна

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері журналістики.

Загальні

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК08. Здатність спілкуватися з представниками інших професійних груп різного рівня.

Спеціальні

СК01. Здатність використовувати спеціалізовані концептуальні знання з теорії та історії журналістики, новітні технологічні досягнення для розв’язання задач дослідницького та/або інноваційного характеру у сфері журналістики / медіаправа.

СК02. Здатність критично осмислювати проблеми у сфері журналістики та дотичні до них міждисциплінарні проблеми.

СК05. Здатність зрозуміло і недвозначно доносити власні висновки з питань журналістики, а також знання та пояснення, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, які навчаються.

СК06. Здатність інтегрувати знання та розв’язувати складні задачі журналістики у широких та/або мультидисциплінарних контекстах, за умов неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.

Опанувавши дисципліну «Європейські медійні стандарти» здобувачі освіти повинні володіти такими ***результатами навчання:***

РН01. Приймати ефективні рішення з проблем журналістики, у тому числі в умовах багатокритерійності, неповних чи суперечливих інформації та вимог.

РН05. Генерувати нові ідеї та використовувати сучасні технології під час створення медіапродуктів.

РН08. Використовувати передові знання і методики у процесі дослідження діяльності та створення нових медіаінституцій.

РН10. Мати практичні навички розв’язання проблем, пов’язаних з організацією нових медіаустанов та інституцій.

РН11. Брати продуктивну участь у розробленні проєктів документів, що регламентують діяльність в

усіх сферах журналістики, обґрунтовувати суспільну потребу в їх прийнятті, прогнозувати результати їх впливу на суспільство.

РН14. Приймати рішення та розв'язувати професійні завдання з позицій соціальної відповідальності, верховенства права та дотримання законодавства

1.2. Тематика практичних занять

№	Назва теми	К-сть годин, денна форма	К-сть годин, заочна форма
1	Тема 1: Основи та принципи інформаційної безпеки	4	1
2	Тема 2: Нормативно-правове регулювання інформаційної безпеки	4	1
3	Тема 3: Методи та засоби захисту інформації	4	1
4	Тема 4: Управління ризиками та інцидентами інформаційної безпеки	4	1
5	Тема 5: Захист інформації в різних інформаційних системах та кіберзлочинність	4	2
	Всього	**20**	**6**

1.3. Контрольні заходи та засоби діагностики

Поточний контроль знань студентів з освітньої компоненти проводиться за такими формами:

- оцінювання активності та роботи здобувачів освіти на лекціях;
- усне опитування на практичних заняттях або підготовка, презентація і обговорення укладеного та проаналізованого прикладного матеріалу;
- виконання контрольних або тематичнотворчих робіт та тестових завдань;
- участь в обговоренні проблемних питань / дискусія;
- використовуючи отримані навики практико-орієнтованого навчання крізь аналіз конкретних ситуацій (Case-study) аналітичні доповіді;
- виконання поточних контрольних робіт за темами змістових модулів та тестових завдань.

1.4. Критерії та шкала оцінювання

Основними критеріями, що визначають ступінь компетентності здобувача вищої освіти при оцінюванні результатів поточного контролю з навчальної дисципліни «Медіабезпека та інформаційне суспільство» є:

- дотримання зазначених дедлайнів виконання всіх видів навчально-професійної роботи, зазначених у робочій програмі навчальної дисципліни;
- аналіз теоретико-прикладної складової акумуляції знань навчального матеріалу за змістом навчальної дисципліни, що міститься в основних та додаткових рекомендованих літературних джерелах;
-використання структурних характеристик тематичного діапазону, умов результативності медіа щодо пошуку, оброблення та аналізу інформації;

- використовувати основні поняття та принципи теоретико-методологічних засади журналістської діяльності (мислення, аналіз, синтез);

- вміння застосовувати теоретико-прикладні знання у професійній діяльності;

- вміння використовувати теоретико-прикладні навички аналізу інформаційного простору України щодо особливостей функціонування медіаправового та медіабезпечного середовища.

Оцінювання результатів поточного контролю проводиться у розрахунку від 0 до 60 балів. Основними методами оцінювання є:

- аналіз усних відповідей;
- виконання практичних завдань.

Оцінювання виконання завдань здійснюється за такими критеріями (у % від кількості балів, виділених на завдання із заокругленими до цілого числа):

0% - завдання не виконано;

40% - завдання виконано частково, висновки не аргументовані і не конкретні, звіт підготовлено недбало;

60% - завдання виконано повністю, висновки містять окремі недоліки, судження студента не достатньо аргументовані, звіт підготовлено з незначним відхиленням від вимог;

80% - завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки несистемного характеру;

100% - завдання виконано правильно, вчасно і без зауважень.

Контрольні заходи та засоби діагностики

Поточний контроль знань студентів з навчальної дисципліни проводиться у формах:

- оцінювання роботи студента на лекціях;

- опитування на практичних заняттях;
- опрацювання завдань для самостійної роботи;
- написання модульних контролів.

Шкала оцінювання

Кількість набраних балів студентом	**Оцінка за національною шкалою**
90-100 балів	Відмінно
82-89 балів	Добре
74-81 балів	
64-73 балів	Задовільно
60-63 балів	
35-59 балів	Незадовільно з можливістю повторного складання
1-34 балів	Незадовільно з обов'язковим повторним вивченням курсу

Порядок оцінювання програмних результатів навчання/результатів навчання

Вид занять	Бали	Форма контролю
Поточна складова оцінювання		
Змістовий модуль		
Практичне заняття 1: Основи та принципи інформаційної безпеки Мета: Поглибити розуміння студентами базових концепцій інформаційної	10	***Форми проведення занять*** – практичне заняття ***Методи та***

безпеки та їхньої важливості для сучасного суспільства. Завдання: Обґрунтуйте, чому поняття конфіденційності, цілісності та доступності інформації є взаємопов'язаними і однаково важливими для забезпечення комплексної безпеки. Визначте щонайменше п'ять видів загроз інформаційній безпеці, з якими може зіткнутися типова організація, та наведіть приклади для кожної. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте відомий випадок порушення інформаційної безпеки (наприклад, витік даних великої компанії, атака вірусу-здирника). Запропонуйте першочергові кроки, які мала б зробити організація для мінімізації шкоди та відновлення довіри.		***технології навчання*** – комбіноване практичне заняття: доповіді, повідомлення, які переходять у розгорнуту дискусію в аудиторії. ***Форма контролю*** – підготовка презентації
Практичне заняття 2: Нормативно-правове регулювання інформаційної безпеки Мета: Ознайомити студентів	10	***Форми проведення занять*** – *практичне заняття*

з основними нормативно-правовими актами у сфері інформаційної безпеки та їх застосуванням. Завдання: Обґрунтуйте необхідність гармонізації українського законодавства у сфері захисту персональних даних з міжнародними стандартами, такими як GDPR. Визначте ключові вимоги Закону України «Про основні засади забезпечення кібербезпеки України» до суб'єктів критичної інфраструктури. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте випадок, коли організація зазнала санкцій за недотримання вимог щодо захисту персональних даних (наприклад, згідно з GDPR). Запропонуйте план заходів, які організація мала б вжити, щоб відповідати цим вимогам.		***Методи та технології навчання*** – демонстрація та обговорення ***Форма контролю*** – практичне заняття з виступами студентів
Практичне заняття 3: **Методи та засоби захисту інформації** **Мета**: Навчити студентів	**10**	***Форми проведення занять*** – *практичне*

розрізняти та застосовувати різні методи і засоби захисту інформації. **Завдання**: Обґрунтуйте, чому використання лише програмних засобів захисту (наприклад, антивірусу) недостатньо для забезпечення комплексної інформаційної безпеки. Визначте основні переваги та недоліки симетричного та асиметричного шифрування та наведіть приклади їх застосування. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте сценарій кібератаки на корпоративну мережу (наприклад, фішинг, DDoS-атака). Запропонуйте комбінацію організаційних та технічних засобів захисту, яка могла б запобігти або мінімізувати наслідки такої атаки.		*заняття* ***Методи та технології навчання*** *– демонстрація* ***Форма контролю*** *– групове опитування студентів*
Практичне заняття 4: Управління ризиками та інцидентами інформаційної безпеки Мета: Розвинути у студентів навички ідентифікації	**10**	***Форми проведення занять*** *– практичне заняття* ***Методи та***

ризиків, розробки політик безпеки та реагування на інциденти. Завдання: Обґрунтуйте важливість проактивного управління ризиками інформаційної безпеки порівняно з реагуванням на вже існуючі загрози. Визначте ключові етапи плану реагування на інцидент інформаційної безпеки (наприклад, виявлення, локалізація, усунення, відновлення). Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте гіпотетичний інцидент, пов'язаний з витоком конфіденційної інформації з компанії. Запропонуйте дії для команди безпеки відповідно до етапів реагування на інцидент.		***технології навчання*** – *демонстрація* ***Форма контролю*** – *групове опитування студентів*
Практичне заняття 5: Захист інформації в різних інформаційних системах та кіберзлочинність Мета: Ознайомити студентів з особливостями захисту інформації в різних	**10**	***Форми проведення занять*** – *практичне заняття* ***Методи та технології***

інформаційних системах та основними аспектами кіберзлочинності. Завдання: Обґрунтуйте, чому безпека мобільних додатків вимагає особливого підходу порівняно з безпекою традиційних веб-ресурсів. Визначте основні види загроз для хмарних сервісів та запропонуйте методи їх мінімізації. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте реальний випадок кіберзлочину (наприклад, фінансове шахрайство через інтернет, злам акаунтів). Запропонуйте превентивні заходи для користувачів та організацій, а також перші кроки у випадку виявлення подібного злочину.		***навчання*** *– демонстрація презентації та аналіз конкретних ситуацій* ***Форма контролю*** *– обговорення кейсів*
Усього практичні заняття	**50**	
Індивідуальне науково-дослідне завдання	**10**	Наукова стаття, або тези або реферат.
Усього поточна складова оцінювання:	60	
Підсумкова складова оцінювання		

2.1 Модульний контроль №1	20	Тести
2.2 Модульний контроль №2	20	Тести
Усього підсумкова складова оцінювання:	40	
РАЗОМ	**100**	

2. ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1: Основи та принципи інформаційної безпеки

1. Поняття інформаційної безпеки: конфіденційність, цілісність, доступність.
2. Класифікація загроз інформаційній безпеці: випадкові, навмисні, зовнішні, внутрішні.

Основні принципи побудови системи захисту інформації.

Мета: Мета: Поглибити розуміння студентами базових концепцій інформаційної безпеки та їхньої важливості для сучасного суспільства.

Теоретична частина (для самостійного опрацювання перед заняттям)

Перед початком практичного заняття студентам рекомендується повторити матеріали лекцій, присвячені фундаментальним концепціям інформаційної безпеки: конфіденційність, цілісність, доступність (тріада CIA). Ознайомтеся з різними класифікаціями загроз інформаційній безпеці (природні, техногенні, навмисні, випадкові) та їхніми потенційними наслідками для організацій та приватних осіб.

Завдання для виконання на практичному занятті:

1. Обґрунтування взаємопов'язаності конфіденційності, цілісності та доступності

Завдання: Обґрунтуйте, чому поняття конфіденційності, цілісності та доступності інформації є взаємопов'язаними і однаково важливими для забезпечення комплексної безпеки.

Методичні рекомендації:

Дайте чітке визначення кожного з трьох принципів (конфіденційність, цілісність, доступність).

Поясніть, як порушення одного з принципів може призвести до компрометації інших. Наприклад:

Як порушення доступності (DDoS-атака) може вплинути на цілісність (неможливість оновлення даних) або конфіденційність (у разі, якщо відмову в обслуговуванні використовують для відволікання уваги від витоку).

Як порушення конфіденційності (витік даних) може підірвати цілісність (втрата довіри до даних) і доступність (неможливість використання скомпрометованих систем).

Як порушення цілісності (зміна даних) може вплинути на доступність (дані стають непридатними для використання) і конфіденційність (скомпрометовані дані можуть містити чутливу інформацію).

Наведіть конкретні приклади з різних сфер (банківська система, медичні дані, державні реєстри), де порушення будь-якого з цих принципів мало б критичні наслідки.

Підкресліть, що справжня безпека досягається лише тоді, коли всі три компоненти розглядаються як єдине ціле.

2. Визначення видів загроз інформаційній безпеці

Завдання: Визначте щонайменше п'ять видів загроз інформаційній безпеці, з якими може зіткнутися типова організація, та наведіть приклади для кожної.

Методичні рекомендації:

Складіть список загроз, що охоплюють різні аспекти (технічні, людські, природні тощо). Розгляньте такі категорії загроз:

Шкідливе програмне забезпечення (Malware): Віруси, трояни, черв'яки, віруси-здирники (ransomware). Приклад: атака вірусу-здирника WannaCry на медичні установи.

Соціальна інженерія: Фішинг, вішинг (голосовий фішинг), смішинг (SMS-фішинг), претекстинг. Приклад: співробітник отримує підроблений лист від «директора» з вимогою перевести кошти.

Несанкціонований доступ: Злом паролів, використання вразливостей ПЗ, інсайдерські загрози. Приклад: колишній співробітник отримує доступ до корпоративної мережі через не видалений обліковий запис.

Відмова в обслуговуванні (DoS/DDoS-атаки): Перевантаження серверів запитами. Приклад: блокування роботи веб-сайту банку під час пікового навантаження.

Витоки даних: Втрата/крадіжка носіїв інформації, публікація конфіденційних даних через помилку, злочинний умисел. Приклад: втрата ноутбука з персональними даними клієнтів у громадському місці.

(Додатково, якщо дозволяє час): Людські помилки, природні катастрофи, апаратні збої, прослуховування.

Для кожного виду загрози наведіть чіткий, зрозумілий приклад, що демонструє її суть та потенційні наслідки для організації.

Аналіз конкретних ситуацій (Case-study):

Завдання: Проаналізуйте відомий випадок порушення інформаційної безпеки (наприклад, витік даних великої компанії, атака вірусу-здирника). Запропонуйте першочергові кроки, які мала б зробити організація для мінімізації шкоди та відновлення довіри.

Методичні рекомендації:

Студенти працюють у малих групах (3-4 особи). Кожна група обирає або отримує для аналізу конкретний відомий кейс (наприклад, витік даних Equifax, атака на Colonial Pipeline, злам Sony Pictures, або інший резонансний випадок).

Етапи аналізу:

Короткий опис інциденту: Що сталося, коли, як і які були безпосередні наслідки (яка інформація скомпрометована, які системи постраждали, фінансові втрати).

Ідентифікація типу загрози та вразливості: Який саме вид атаки був використаний? Які слабкі місця в системі безпеки організації дозволили цьому статися?

Розробка першочергових кроків реагування: Запропонуйте дії, які організація мала б негайно вжити для:

Локалізації інциденту: Відключення скомпрометованих систем, ізоляція заражених сегментів мережі.

Оцінки масштабу: Визначення обсягу витоку даних, кількості постраждалих користувачів/систем.

Сповіщення: Інформування відповідних органів (правоохоронні органи, регулятори), клієнтів, партнерів.

Запобігання подальшій шкоді: Зміна паролів, відкликання скомпрометованих сертифікатів, оновлення патчів.

Комунікації: Розробка публічного звернення, робота зі ЗМІ для відновлення довіри.

Початок розслідування: Залучення фахівців з кібербезпеки.

Презентація результатів: Кожна група презентує свій аналіз та запропоновані кроки. Після презентації відбувається спільне обговорення та конструктивна критика.

Запитання для обговорення та висновки:

Чому знання основних принципів та загроз є фундаментом для будь-якої подальшої роботи в інформаційній безпеці?

Які фактори найчастіше призводять до успішних кібератак (людський фактор, технічні вразливості, відсутність політик)?

Як важливо, щоб усі співробітники організації розуміли базові принципи інформаційної безпеки?

Які висновки можна зробити щодо важливості проактивного підходу до інформаційної безпеки?

Форма контролю: Підготовка презентації.

Тема 2: Нормативно-правове регулювання інформаційної безпеки

1. Законодавство України у сфері інформаційної та кібербезпеки: ключові закони та нормативні акти.
2. Міжнародні стандарти та рекомендації з інформаційної безпеки (ISO 27001, NIST).
3. Правові аспекти захисту персональних даних (GDPR) та критичної інфраструктури.

Мета: Ознайомити студентів з основними нормативно-правовими актами у сфері інформаційної безпеки та їх застосуванням.

Теоретична частина (для самостійного опрацювання перед заняттям)

Перед початком практичного заняття студентам рекомендується повторити матеріали лекцій, присвячені ключовим міжнародним стандартам у сфері захисту персональних даних (зокрема GDPR – General Data Protection Regulation), а також основному українському законодавству, що регулює інформаційну безпеку (Закони України «Про інформацію», «Про захист персональних даних», «Про електронні довірчі послуги», «Про основні засади забезпечення кібербезпеки України»). Зверніть особливу увагу на принципи обробки персональних даних та вимоги до суб'єктів критичної інфраструктури.

Завдання для виконання на практичному занятті:

1. Обґрунтування необхідності гармонізації українського законодавства з міжнародними стандартами

Завдання: Обґрунтуйте необхідність гармонізації українського законодавства у сфері захисту персональних даних з міжнародними стандартами, такими як GDPR.

Методичні рекомендації:

Поясніть, що таке GDPR (Загальний регламент про захист даних ЄС) та чому він став глобальним стандартом.

Розгляньте основні принципи GDPR (законність, справедливість та прозорість; обмеження мети; мінімізація даних; точність; обмеження зберігання; цілісність та конфіденційність; підзвітність).

Обговоріть переваги гармонізації для України:

Сприяння європейській інтеграції та цифровій трансформації.

Підвищення довіри міжнародних партнерів та інвесторів до українських компаній.

Можливість для українських компаній працювати на ринку ЄС без додаткових регуляторних бар'єрів.

Посилення захисту прав та свобод громадян України щодо їхніх персональних даних.

Забезпечення відповідності міжнародним зобов'язанням.

Наведіть приклади, коли відсутність гармонізації створювала проблеми для українських організацій або громадян.

2. Визначення ключових вимог Закону України «Про основні засади забезпечення кібербезпеки України»

Завдання: Визначте ключові вимоги Закону України «Про основні засади забезпечення кібербезпеки України» до суб'єктів критичної інфраструктури.

Методичні рекомендації:

Поясніть, хто є суб'єктами критичної інфраструктури згідно із Законом (наприклад, об'єкти енергетики, транспорту, фінансового сектору, телекомунікацій тощо). Обґрунтуйте, чому саме ці об'єкти потребують посиленого захисту.

Перерахуйте та розкрийте основні вимоги, що висуваються до цих суб'єктів, наприклад:

Розробка та впровадження систем управління інформаційною безпекою.

Регулярне проведення аудитів та тестування на проникнення.

Створення підрозділів з кібербезпеки або призначення відповідальних осіб.

Оперативне реагування на кіберінциденти та взаємодія з Національним координаційним центром кібербезпеки (НКЦК).

Забезпечення стійкості та безперервності функціонування інформаційних систем.

Підвищення кваліфікації персоналу з питань кібербезпеки.

Обговоріть, як невиконання цих вимог може вплинути на національну безпеку та функціонування держави.

Аналіз конкретних ситуацій (Case-study):

Завдання: Проаналізуйте випадок, коли організація зазнала санкцій за недотримання вимог щодо захисту персональних даних (наприклад, згідно з GDPR). Запропонуйте план заходів, які організація мала б вжити, щоб відповідати цим вимогам.

Методичні рекомендації:

Студенти працюють у малих групах (3-4 особи). Кожна група обирає або отримує для аналізу реальний відомий кейс порушення GDPR (наприклад, штрафи Google, British Airways, Marriott International, або інші резонансні випадки).

Етапи аналізу:

Короткий опис кейсу: Яка компанія, за що саме була оштрафована/зазнала санкцій, який розмір штрафу, які були наслідки.

Визначення порушених норм GDPR (або іншого релевантного законодавства): Які саме принципи або статті регламенту були порушені організацією? (Наприклад, відсутність згоди на обробку, неналежний захист, несвоєчасне повідомлення про витік).

Розробка плану заходів відповідності: Запропонуйте конкретний, покроковий план дій, який організація мала б вжити для уникнення подібних порушень у майбутньому та забезпечення відповідності вимогам захисту даних. План може включати:

Проведення аудиту: Визначення типів персональних даних, що обробляються, їхніх потоків, місць зберігання.

Розробка політик: Впровадження або оновлення політик конфіденційності, політик захисту даних, інструкцій для працівників.

Призначення відповідальних: Призначення спеціаліста із захисту даних (DPO), формування команди.

Технічні заходи: Шифрування, псевдонімізація даних, контроль доступу, резервне копіювання, регулярні оновлення.

Навчання персоналу: Проведення регулярних тренінгів для всіх співробітників щодо важливості захисту даних та їхніх обов'язків.

Взаємодія з суб'єктами даних: Забезпечення права на доступ, виправлення, видалення даних.

Процедури реагування на інциденти: Розробка плану дій у разі витоку даних.

Презентація результатів: Кожна група презентує свій аналіз та запропонований план заходів. Після презентації відбувається спільне обговорення та конструктивна критика.

Запитання для обговорення та висновки:

Чому міжнародне співробітництво у сфері кібербезпеки є настільки важливим?

Які виклики постають перед Україною в процесі імплементації міжнародних стандартів кібербезпеки та захисту даних?

Яка роль кожного співробітника організації у дотриманні вимог нормативно-правових актів у сфері інформаційної безпеки?

Наскільки суворими, на вашу думку, мають бути покарання за порушення вимог щодо захисту персональних даних?

Форма контролю: Практичне заняття з виступами студентів.

Тема 3: Методи та засоби захисту інформації

1. Криптографічні методи захисту інформації: шифрування, електронний підпис, хешування.
2. Організаційні та технічні засоби захисту: розмежування доступу, автентифікація, фаєрволи, системи виявлення вторгнень.

Програмне та апаратне забезпечення для захисту інформації: антивіруси, системи резервного копіювання, VPN.

Мета: Навчити студентів розрізняти та застосовувати різні методи і засоби захисту інформації.

Теоретична частина (для самостійного опрацювання перед заняттям)

Перед початком практичного заняття студентам рекомендується повторити матеріали лекцій, що стосуються класифікації методів та засобів захисту інформації (організаційні, програмні, технічні, криптографічні). Особливу увагу приділіть принципам роботи симетричного та асиметричного шифрування,

їхнім перевагам, недолікам та типовим сценаріям застосування. Ознайомтеся з основами функціонування антивірусних програм, міжмережевих екранів (файрволів) та систем виявлення/запобігання вторгненням (IDS/IPS).

Завдання для виконання на практичному занятті:

1. Обґрунтування недостатності лише програмних засобів захисту

Завдання: Обґрунтуйте, чому використання лише програмних засобів захисту (наприклад, антивірусу) недостатньо для забезпечення комплексної інформаційної безпеки.

Методичні рекомендації:

Поясніть, що програмні засоби є важливою, але лише частиною комплексної системи безпеки.

Наведіть обмеження програмних засобів:

Не покривають усі види загроз: Антивірус захищає переважно від відомих шкідливих програм, але не від соціальної інженерії, інсайдерських загроз, фізичного доступу чи виходу з ладу апаратного забезпечення.

Залежність від оновлень: Ефективність програм залежить від своєчасного оновлення баз даних та сигнатур. Нові загрози можуть обходити захист.

Вразливості в самому ПЗ: Програмні засоби також можуть мати вразливості, які можуть бути використані зловмисниками.

Не враховують людський фактор: Програмне забезпечення не може повністю компенсувати помилки користувачів або їхню необережність (наприклад, перехід за фішинговим посиланням).

Обґрунтуйте необхідність інтеграції з іншими видами захисту:

Організаційні: Політики безпеки, навчання персоналу, розподіл повноважень.

Технічні (апаратні): Міжмережеві екрани (hardware firewall), системи контролю доступу, фізичний захист серверних приміщень.

Криптографічні: Шифрування даних.

Наведіть гіпотетичні або реальні приклади, де лише програмний захист виявився неефективним.

2. Переваги та недоліки симетричного та асиметричного шифрування

Завдання: Визначте основні переваги та недоліки симетричного та асиметричного шифрування та наведіть приклади їх застосування.

Методичні рекомендації:

Симетричне шифрування:

Принцип: Один ключ використовується як для шифрування, так і для розшифрування.

Переваги: Висока швидкість шифрування, менші обчислювальні витрати, добре підходить для шифрування великих обсягів даних.

Недоліки: Проблема безпечної передачі ключа між сторонами; складність управління ключами у великих мережах (N(N-1)/2 ключів).

Приклади застосування: Шифрування файлів на диску (BitLocker, AES-256), SSL/TLS-з'єднання (сама передача даних після обміну ключами), VPN-тунелі.

Асиметричне шифрування (криптографія з відкритим ключем):

Принцип: Використання пари ключів – відкритого (public key) для шифрування/перевірки підпису та закритого (private key) для розшифрування/формування підпису.

Переваги: Вирішує проблему обміну ключами, дозволяє реалізувати цифрові підписи, аутентифікацію, невідмовність.

Недоліки: Значно повільніше симетричного, більші обчислювальні витрати, тому не використовується для прямого шифрування великих обсягів даних.

Приклади застосування: Обмін ключами для симетричного шифрування (RSA, Diffie-Hellman), цифрові підписи (електронний цифровий підпис), захист електронної пошти (PGP), автентифікація на веб-сайтах (TLS/SSL Handshake).

Підкресліть, що на практиці часто використовується гібридна система, де асиметричне шифрування застосовується для безпечного обміну ключами, а симетричне – для шифрування самих даних.

Аналіз конкретних ситуацій (Case-study):

Завдання: Проаналізуйте сценарій кібератаки на корпоративну мережу (наприклад, фішинг, DDoS-атака). Запропонуйте комбінацію організаційних та технічних засобів захисту, яка могла б запобігти або мінімізувати наслідки такої атаки.

Методичні рекомендації:

Студенти працюють у малих групах (3-4 особи). Кожна група обирає або отримує для аналізу один зі сценаріїв атаки (наприклад, успішна фішингова атака, що призвела до компрометації облікових даних; або DDoS-атака, що паралізувала роботу веб-сервісу).

Етапи аналізу та розробки плану захисту:

Детальний опис сценарію: Які кроки були зроблені зловмисником? Які вразливості були використані? Які потенційні наслідки?

Ідентифікація типу загрози та її вектора: Визначте, який тип кібератаки відбувається (наприклад, соціальна інженерія через електронну пошту, атака на доступність).

Розробка комбінованого плану захисту: Запропонуйте конкретні заходи, розділені за категоріями:

Організаційні засоби:

Навчання персоналу (регулярні тренінги з кібергігієни, симуляції фішингу).

Розробка та впровадження чітких політик безпеки (політика паролів, політика використання ресурсів, політика реагування на інциденти).

Розподіл обов'язків та відповідальності за безпеку.

Контроль фізичного доступу до обладнання.

Технічні засоби (програмні та апаратні):

Антивірусне та анти-шкідливе ПЗ: На всіх пристроях, з регулярними оновленнями.

Міжмережеві екрани (Firewall): На периметрі мережі та на кінцевих точках.

Системи виявлення/запобігання вторгнень (IDS/IPS): Моніторинг трафіку на аномалії.

Системи фільтрації контенту: Для електронної пошти та веб-трафіку (блокування шкідливих посилань/вкладень).

Багатофакторна автентифікація (MFA): Для всіх критичних систем та акаунтів.

Системи резервного копіювання: Регулярне та безпечне створення резервних копій.

Оновлення ПЗ та системи: Регулярне застосування патчів безпеки.

Системи управління інформацією про безпеку та подіями (SIEM): Для централізованого збору та аналізу журналів.

VPN: Для захищеного доступу до корпоративних ресурсів ззовні.

Засоби криптографічного захисту: Шифрування даних на дисках, в базах даних, при передачі.

Презентація результатів: Кожна група презентує свій аналіз сценарію та запропонований комплексний план захисту. Після презентації відбувається спільне обговорення та конструктивна критика.

Запитання для обговорення та висновки:

Наскільки ефективним може бути захист інформації, якщо ігнорується хоча б один з видів засобів захисту (організаційний, технічний, криптографічний)?

Яку роль відіграє «людський фактор» у ефективності застосування технічних засобів захисту?

Які нові технології (наприклад, штучний інтелект) можуть бути використані для посилення або, навпаки, для обходу існуючих засобів захисту?

Чому постійне оновлення та моніторинг є критично важливими для ефективності засобів захисту?

Форма контролю: Групове опитування студентів.

Тема 4: Управління ризиками та інцидентами інформаційної безпеки

1. Методології оцінки ризиків інформаційної безпеки: ідентифікація, аналіз, оцінка та мінімізація.

2. Розробка політик інформаційної безпеки та планів реагування на інциденти.

3. Аудит та моніторинг інформаційної безпеки: цілі, методи та інструменти.

Мета: Розвинути у студентів навички ідентифікації ризиків, розробки політик безпеки та реагування на інциденти.

Теоретична частина (для самостійного опрацювання перед заняттям)

Перед початком практичного заняття студентам рекомендується повторити матеріали лекцій, присвячені методологіям управління ризиками інформаційної безпеки (ідентифікація, оцінка, обробка, моніторинг ризиків). Особливу увагу приділіть етапам плану реагування на інциденти (Incident Response Plan - IRP): виявлення, локалізація, усунення, відновлення, аналіз після інциденту. Ознайомтеся з поняттям політик інформаційної безпеки та їхньою роллю в системі менеджменту безпеки.

Завдання для виконання на практичному занятті:

1. Обґрунтування важливості проактивного управління ризиками

Завдання: Обґрунтуйте важливість проактивного управління ризиками інформаційної безпеки порівняно з реагуванням на вже існуючі загрози.

Методичні рекомендації:

Поясніть різницю між проактивним (превентивним) та реактивним підходами до безпеки.

Наведіть аргументи на користь проактивного підходу:

Економія ресурсів: Запобігання інцидентам завжди дешевше, ніж ліквідація їхніх наслідків (фінансові втрати, репутаційні збитки, юридичні витрати).

Зниження ймовірності інцидентів: Систематичне виявлення та усунення вразливостей до того, як їх використають зловмисники.

Підвищення стійкості: Організація краще підготовлена до можливих атак, що забезпечує безперервність її роботи.

Збереження репутації та довіри: Запобігання витокам даних та збоям підтримує імідж компанії та довіру клієнтів.

Дотримання нормативних вимог: Багато регуляцій вимагають саме проактивного підходу до безпеки.

Наведіть конкретні приклади, коли відсутність проактивного управління призводила до серйозних інцидентів (наприклад, використання відомих, але не усунених вразливостей).

Обговоріть роль регулярних аудитів, тестування на проникнення та оцінки ризиків у проактивному підході.

2. Визначення ключових етапів плану реагування на інцидент

Завдання: Визначте ключові етапи плану реагування на інцидент інформаційної безпеки (наприклад, виявлення, локалізація, усунення, відновлення).

Методичні рекомендації:

Розкрийте зміст кожного етапу, який зазвичай включає:

Підготовка (Preparation): До інциденту. Розробка політик, навчання команди, наявність інструментів, створення плану, резервні копії.

Виявлення та аналіз (Identification & Analysis): Визначення інциденту, збір інформації, оцінка масштабу, визначення типу атаки.

Локалізація (Containment): Ізоляція скомпрометованих систем/даних, зупинка поширення інциденту, відключення мереж, блокування облікових записів.

Усунення (Eradication): Видалення причини інциденту (шкідливе ПЗ, вразливості), очищення систем, виключення повторного зараження.

Відновлення (Recovery): Відновлення систем з резервних копій, повернення до нормальної роботи, моніторинг.

Аналіз після інциденту (Post-incident Activity/Lessons Learned): Документування інциденту, виявлення причинно-наслідкових зв'язків, оновлення політик та процедур, навчання персоналу для запобігання подібним інцидентам у майбутньому.

Наведіть короткі приклади дій, які виконуються на кожному етапі.

Підкресліть, що ці етапи не завжди є лінійними, іноді доводиться повертатися на попередні фази.

Аналіз конкретних ситуацій (Case-study):

Завдання: Проаналізуйте гіпотетичний інцидент, пов'язаний з витоком конфіденційної інформації з компанії. Запропонуйте дії для команди безпеки відповідно до етапів реагування на інцидент.

Методичні рекомендації:

Студенти працюють у малих групах (3-4 особи). Кожна група отримує для аналізу гіпотетичний сценарій витоку даних, наприклад:

Сценарій: Співробітник випадково публікує таблицю з персональними даними клієнтів на публічному хмарному сховищі.

Сценарій: Зовнішній зловмисник отримує доступ до бази даних компанії через вразливість у веб-додатку і викрадає конфіденційні дані.

Сценарій: Інсайдер навмисно копіює та виносить комерційну таємницю.

Етапи аналізу та розробки плану реагування:

Опис інциденту: Детально опишіть, що сталося, яка інформація скомпрометована, які потенційні наслідки.

Застосування етапів реагування на інцидент: Покроково розпишіть дії, які команда безпеки має вжити на кожному з визначених раніше етапів (виявлення, локалізація, усунення, відновлення, аналіз після інциденту).

Приклад для сценарію «випадкова публікація»:

Виявлення: Моніторинг публічних ресурсів, оповіщення від пильних користувачів/регуляторів.

Локалізація: Негайне видалення файлу з публічного сховища, відкликання посилань, блокування доступу.

Усунення: Встановлення причини (людська помилка, відсутність контролю), впровадження DLP-систем (Data Loss Prevention), посилення політик.

Відновлення: Перевірка, чи не було інших копій, відновлення довіри клієнтів через публічне сповіщення та компенсації (за потреби).

Аналіз: Перегляд процедур, навчання співробітників, оновлення правил доступу до даних.

Презентація результатів: Кожна група презентує свій сценарій та розроблений план дій. Після презентації відбувається спільне обговорення та конструктивна критика.

Запитання для обговорення та висновки:

Наскільки ефективним є реагування на інцидент без попередньої підготовки та розробленого плану?

Яку роль відіграє комунікація (внутрішня та зовнішня) під час інциденту безпеки?

Чому етап «аналізу після інциденту» є не менш важливим, ніж сам процес локалізації та усунення?

Які фактори можуть ускладнити або уповільнити процес реагування на інцидент?

Форма контролю: Групове опитування студентів.

Тема 5: Захист інформації в різних інформаційних системах та кіберзлочинність

1. Особливості захисту інформації в комп'ютерних мережах та хмарних сервісах.
2. Безпека веб-ресурсів та мобільних додатків.
3. Кіберзлочинність: види, методи протидії та розслідування кіберзлочинів.

Мета: Мета: Ознайомити студентів з особливостями захисту інформації в різних інформаційних системах та основними аспектами кіберзлочинності.

Теоретична частина (для самостійного опрацювання перед заняттям)

Перед початком практичного заняття студентам рекомендується повторити матеріали лекцій, що стосуються архітектури та особливостей безпеки різних інформаційних систем: мобільних додатків, хмарних сервісів, Інтернету речей (IoT). Ознайомтеся з основними видами кіберзлочинів (фінансове шахрайство, крадіжка даних, вимагання, кібершпигунство, кібертероризм) та методами їх реалізації. Дослідіть принципи роботи мобільних операційних систем (Android, iOS) та хмарних платформ (AWS, Azure, Google Cloud) з точки зору безпеки.

Завдання для виконання на практичному занятті:

1. Обґрунтування особливого підходу до безпеки мобільних додатків

Завдання: Обґрунтуйте, чому безпека мобільних додатків вимагає особливого підходу порівняно з безпекою традиційних веб-ресурсів.

Методичні рекомендації:

Визначте ключові відмінності мобільних додатків від веб-ресурсів, які створюють унікальні виклики для безпеки:

Середовище виконання: Мобільні пристрої часто використовуються в неконтрольованих мережах (публічний Wi-Fi), є більш схильними до фізичної втрати/крадіжки.

Доступ до ресурсів пристрою: Мобільні додатки часто мають доступ до камери, мікрофона, геолокації, контактів, SMS, що створює ризики приватності та витоку даних.

Фрагментація ОС та пристроїв: Велика кількість версій ОС Android та різноманітність пристроїв ускладнює стандартизацію безпеки та випуск оновлень.

Магазини додатків: Хоча магазини (Google Play, App Store) перевіряють додатки, шкідливі програми все ж можуть проникати.

Розробка: Часто розробники мобільних додатків можуть не приділяти достатньої уваги безпеці на етапі кодування.

Обмежені ресурси: Мобільні пристрої мають обмежені обчислювальні можливості та заряд батареї, що впливає на вибір криптографічних алгоритмів та інших засобів захисту.

Наведіть приклади специфічних загроз для мобільних додатків (шкідливі додатки, небезпечні

дозволи, незахищене зберігання даних, MITM-атаки в мобільних мережах).

Обґрунтуйте, що для мобільних додатків потрібен комплексний підхід, що включає безпечну розробку (Secure SDLC), тестування на проникнення, управління дозволами та шифрування даних.

2. Визначення основних видів загроз для хмарних сервісів

Завдання: Визначте основні види загроз для хмарних сервісів та запропонуйте методи їх мінімізації.

Методичні рекомендації:

Поясніть, що таке хмарні сервіси (IaaS, PaaS, SaaS) та чому вони стали популярними.

Визначте основні загрози, специфічні для хмарних середовищ:

Ненадійний контроль доступу та ідентифікації: Слабка автентифікація, несанкціонований доступ до хмарних ресурсів. Метод мінімізації: MFA, принцип найменших привілеїв, регулярний аудит прав доступу.

Витік даних: Через неправильну конфігурацію, зламані API, інсайдерські загрози. Метод мінімізації: шифрування даних (у стані спокою та під час передачі), DLP-системи, моніторинг активності.

Вразливості в API: Незахищені або погано розроблені інтерфейси програмування додатків. Метод мінімізації: безпечна розробка API, API Gateway, регулярне тестування.

Відмова в обслуговуванні (DoS/DDoS): Атаки на хмарну інфраструктуру. Метод мінімізації: використання вбудованих засобів захисту хмарних провайдерів, географічна розподіленість.

Зловживання хмарними сервісами: Використання хмарної інфраструктури для кібератак

(наприклад, хостинг шкідливого ПЗ). Метод мінімізації: моніторинг активності, співпраця з провайдером.

Проблема «спільної відповідальності»: Нерозуміння, за які аспекти безпеки відповідає провайдер, а за які – клієнт. Метод мінімізації: чітке розуміння угоди про рівень обслуговування (SLA) та моделі спільної відповідальності.

Для кожної загрози запропонуйте конкретні методи мінімізації.

Аналіз конкретних ситуацій (Case-study):

Завдання: Проаналізуйте реальний випадок кіберзлочину (наприклад, фінансове шахрайство через інтернет, злам акаунтів). Запропонуйте превентивні заходи для користувачів та організацій, а також перші кроки у випадку виявлення подібного злочину.

Методичні рекомендації:

Студенти працюють у малих групах (3-4 особи). Кожна група обирає або отримує для аналізу реальний відомий кейс кіберзлочину (наприклад, фішингова атака на банківські клієнти, злам відомого акаунта в соціальних мережах, атака вірусу-здирника на малий бізнес, викрадення криптовалюти).

Етапи аналізу та розробки плану:

Короткий опис кіберзлочину: Що сталося, як було реалізовано, які були наслідки для жертви (фінансові, репутаційні, втрата даних).

Ідентифікація використаних методів: Які технічні, соціально-інженерні чи інші методи були застосовані зловмисниками?

Розробка превентивних заходів: Запропонуйте конкретні дії, які могли б запобігти цьому злочину. Розділіть їх на:

Для користувачів: Навчання кібергігієні, використання складних паролів та MFA, обережність при відкритті посилань/вкладень, перевірка джерела інформації, використання ліцензійного ПЗ, регулярне оновлення пристроїв.

Для організацій: Впровадження політик безпеки, навчання персоналу, технічні засоби захисту (файрволи, антивіруси, IDS/IPS), регулярні аудити безпеки, сегментація мережі, резервне копіювання, план реагування на інциденти.

Визначення перших кроків у випадку виявлення злочину: Що робити, якщо злочин вже стався?

Негайна реакція: Відключення скомпрометованих пристроїв/систем, зміна паролів, блокування карток/рахунків.

Збір доказів: Збереження логів, скріншотів, повідомлень, що можуть бути використані для розслідування.

Повідомлення: Звернення до правоохоронних органів (кіберполіції), банку, провайдера послуг, адміністрації платформи.

Інформування: Повідомлення відповідних осіб в організації (керівництво, IT-відділ).

Відновлення: Відновлення систем з резервних копій, очищення від шкідливого ПЗ.

Презентація результатів: Кожна група презентує свій аналіз кейсу та запропоновані заходи. Після презентації відбувається спільне обговорення та конструктивна критика.

Запитання для обговорення та висновки:

Наскільки швидко розвиваються методи кіберзлочинності та як це впливає на необхідність постійного оновлення знань та засобів захисту?

Яку роль відіграє міжнародне співробітництво у боротьбі з кіберзлочинністю?

Чи можливо повністю убезпечити себе та свої дані в сучасному цифровому світі?

Які етичні аспекти виникають у контексті кіберзлочинності (наприклад, відстеження зловмисників, використання «білих хакерів»)?

Форма контролю: Обговорення кейсів.

3. САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота є критично важливою для успішного засвоєння дисципліни «Інформаційна безпека». Вона не лише поглиблює ваші теоретичні знання, а й формує практичні навички та системне мислення, необхідні для ефективного захисту інформації в сучасному цифровому світі. Сфера інформаційної безпеки постійно розвивається, тому ваша здатність до самонавчання та адаптації до нових викликів стане вашою конкурентною перевагою.

Ці рекомендації допоможуть вам максимально ефективно організувати свій навчальний процес.

1. Планування та організація навчання

Створіть власний графік: Розробіть детальний план самостійної роботи, враховуючи теми лекцій, практичних завдань та терміни їх виконання. Дотримуйтеся регулярності — краще вивчати потроху щодня, ніж намагатися освоїти все в останній момент.

Визначте ключові цілі: Перед початком вивчення нової теми чітко сформулюйте, які основні концепції та навички ви повинні опанувати.

Використовуйте різноманітні джерела: Не обмежуйтесь лише основним навчальним матеріалом. Активно шукайте додаткові ресурси: фахові статті, вебінари від провідних експертів, подкасти,

відеоуроки, документальні фільми про кібербезпеку.

2. Поглиблене вивчення теоретичного матеріалу

Детальне конспектування: Під час вивчення лекцій та рекомендованої літератури створюйте розгорнуті конспекти. Виділяйте ключові визначення, принципи, класифікації загроз та методи захисту. Використовуйте таблиці, схеми та ментальні карти для візуалізації складної інформації.

Аналіз нормативно-правових актів: Уважно вивчайте Закони України «Про інформацію», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України», а також ознайомтеся з міжнародними стандартами, такими як GDPR. Зробіть виписки з ключових статей, що регулюють відповідальність та вимоги до захисту інформації.

Створення глосарію: Ведіть власний словник термінів, що стосуються інформаційної безпеки (наприклад, IDS/IPS, SIEM, MFA, DDoS, Ransomware, PII, Zero-day exploit), щоб вільно оперувати професійною термінологією.

3. Практичне застосування знань та розвиток навичок

Аналіз реальних інцидентів: Регулярно вивчайте звіти та аналітику про кіберінциденти, витоки даних та кібератаки, що відбуваються у світі та в Україні. Спробуйте самостійно:

Ідентифікувати: Які принципи інформаційної безпеки були порушені (конфіденційність, цілісність, доступність)?

Класифікувати: До якого виду загроз належить інцидент?

Проаналізувати: Які вразливості були використані?

Запропонувати: Які превентивні заходи могли б запобігти цьому інциденту? Які кроки слід було б вжити для реагування?

Освоєння інструментів:

Кібергігієна: Практично налаштуйте двофакторну автентифікацію на всіх своїх онлайн-акаунтах, освойте роботу з менеджерами паролів. Дослідіть принципи роботи та застосування VPN-сервісів та TOR-браузера.

Захист даних: Вивчіть, як безпечно шифрувати файли та папки на вашому пристрої, як видаляти метадані з документів та зображень.

Ознайомлення з базовими рішеннями: Дослідіть принципи функціонування антивірусних програм, міжмережевих екранів, можливостей операційних систем щодо безпеки.

Симуляції та моделювання: Уявіть себе співробітником відділу безпеки: як би ви діяли у випадку фішингової атаки на вашу компанію? Як би ви розробляли політику використання мобільних пристроїв? Це допоможе закріпити алгоритми дій.

4. Використання додаткових ресурсів та спілкування

Слідкуйте за експертами та організаціями: Підпишіться на блоги, канали та розсилки відомих фахівців з кібербезпеки, а також профільних організацій (наприклад, CERT-UA, SANS Institute, OWASP, Kaspersky).

Онлайн-курси: Проходьте додаткові онлайн-курси з інформаційної безпеки на таких платформах, як Coursera, Prometheus, Udemy, Cybrary.

Професійні спільноти: Долучайтеся до онлайн-форумів та спільнот, де обговорюються актуальні проблеми кібербезпеки, обмінюйтеся досвідом та

ставте запитання.

5. Рефлексія та самооцінка

Ведіть навчальний журнал: Записуйте свої спостереження, висновки, успіхи та труднощі. Це допоможе вам відстежувати свій прогрес.

Самотестування: Після вивчення кожної теми або розділу спробуйте відповісти на питання для самоконтролю. Це дозволить виявити прогалини у знаннях та повернутися до їх поглиблення.

Пам'ятайте, що інформаційна безпека – це безперервний процес навчання та вдосконалення. Ваша проактивність у самостійній роботі стане запорукою вашого успіху в цій динамічній та надзвичайно важливій сфері.

4. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальне науково-дослідне завдання	**20**	Наукова стаття, або тези або реферат.

Написання реферату

Індивідуальне завдання передбачає написання наукової статті, або тези або реферату щодо тематики медіабезпеки та інформаційного суспільства та передбачає дослідження основних питань програмного матеріалу.

Усі реферати/тези/статті повинні відповідати єдиним вимогам https://peremena.com.ua/uk/titul-uk/vimogi-do-referatu-v-ukrayini/ .

Перелік тем для рефератів

1. Тріада CIA (Конфіденційність, Цілісність, Доступність): Взаємозв'язок та практичне

застосування в організації.
2. Соціальна інженерія як основний вектор атак: Види, механізми та методи протидії.
3. Віруси-здирники (Ransomware): Еволюція загроз, наслідки та стратегії захисту.
4. Зловмисне програмне забезпечення (Malware): Класифікація, поширення та виявлення.
5. Внутрішні загрози (Insider Threats): Типи, мотивація та механізми запобігання.
6. Багатофакторна автентифікація (MFA/2FA): Принципи, реалізації та значення для надійного захисту.
7. Криптографічні методи захисту інформації: Порівняльний аналіз симетричного та асиметричного шифрування.
8. Системи виявлення та запобігання вторгненням (IDS/IPS): Принципи роботи та роль у системі безпеки.
9. Управління патчами та оновленнями: Критична необхідність для забезпечення безпеки систем.
10. Політики інформаційної безпеки: Розробка, впровадження та їхня роль у комплексній безпеці.
11. GDPR та захист персональних даних в ЄС: Основні принципи та наслідки для компаній.
12. Закон України «Про основні засади забезпечення кібербезпеки України»: Вимоги та застосування.
13. Управління ризиками інформаційної безпеки: Методології та етапи впровадження.

14. План реагування на інциденти (IRP): Розробка та тестування ефективності.
15. Кіберстрахування: Роль у зниженні фінансових ризиків від кібератак.
16. Безпека хмарних сервісів: Моделі відповідальності та основні загрози.
17. Безпека мобільних додатків: Специфіка загроз та методи захисту.
18. Інтернет речей (IoT) та його вразливості: Виклики для інформаційної безпеки.
19. Види кіберзлочинності: Аналіз сучасних тенденцій та методів боротьби.
20. Кіберрозвідка та кібершпигунство: Методи, цілі та захист від них.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література:

1. Безпека журналістів : збірник документів Ради Європи [Електронний ресурс]. URL: https://rm.coe.int/16806b5970 (дата звернення: 25.08.2023).
2. Кодекс практики Європейського Союзу щодо протидії дезінформації [Електронний ресурс]. URL: https://www.nrada.gov.ua/foreign_practice/ (дата звернення: 25.08.2023).
3. Посібник до навчального курсу щодо безпеки журналістів. Курс розроблено спільно трьома інституціями: Національною школою суддів, Національною академією внутрішніх справ і Тренінговим центром прокурорів України за підтримки Проєкту «Європейський Союз та Рада Європи працюють разом для підтримки свободи медіа в Україні» [Електронний ресурс]. URL:

https://rm.coe.int/bezpekazhurnalistiv-posibnyk-final-print-1-/1680a3f8df (дата звернення: 25.08.2023).

4. Посібник з верифікації : визначний гід з верифікації цифрового контенту для висвітлення надзвичайних подій [Електронний ресурс]. URL: https://verificationhandbook.com/book_ua/chapter8.php (дата звернення: 25.08.2023).

5. Посібник з безпеки для журналістів : посібник для репортерів у небезпечних зонах / Reporters sans frontières (France). 2022 [Електронний ресурс]. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381168 (дата звернення: 25.08.2023).

6. Україна : висвітлення конфлікту в Україні : практичний посібник для журналістів [Електронний ресурс]. URL: https://www.thomsonfoundation.org/media/33402/ukraine1203bleed_ukr_preview.pdf (дата звернення: 25.08.2023).

7. Цифрова безпека журналіста-розслідувача [Електронний ресурс]. URL: https://video.detector.media/lessons/cyfrova-bezpekazhurnalista-rozsliduvacha-i19 (дата звернення: 25.08.2023).

8. Sydorenko N. Improving the Financial Stability of IT Companies through Social Media Marketing / N. Sydorenko, O. Mitchuk, O. Holik, I. Havryliuk, N. Myronets // WSEAS Transactions on Business and Economics. 2022. Vol. 19. P. 1621–1632.

9. Bessarab A. Social networks as a phenomenon of the information society / A. Bessarab, O. Mitchuk, A. Baranetska, O. Kvasnytsia, G. Mykytiv // Journal of Optimization in Industrial Engineering. 2021. Vol. 14, № 1. P. 35–42.

Додаткова література

1. *Безпека інформації* [Електронний ресурс] : навч. посіб. / Ін-т мас. інформації. – Електрон. текст. дані. – Режим доступу: http://imi.org.ua/bezpeka/spravochnik-po-bezopasnosti

2. *Безпека журналістів в Україні: існуючі виклики і шляхи їх подолання* [Електронний ресурс] / Укрінформ. – Електрон. текст. дані. – Режим доступу: https://www.ukrinform.ua/rubric-presshall/3099965-bezpeka-zurnalistiv-v-ukraini-isnuuci-vikliki-ta-slahi-ihpodolanna.html

3. Вальорска М. А. *Діпфейк та дезінформація* [Електронний ресурс] : практ. посіб. / Аґнєшка М. Вальорска ; пер. з нім. В. Олійника. – Київ : Акад. укр. преси ; Центр Вільної Преси, 2020. – 36 с. – Електрон. текст. дані. – Режим доступу: https://www.aup.com.ua/uploads/DEEPFAKES_FNF_AUP_2020.pdf

4. *Верховна Рада посилила відповідальність за злочини проти журналістів* [Електронний ресурс] / Детектор медіа. – Електрон. текст. дані. – Режим доступу: https://detector.media/community/article/184510/2021-02-02-verkhovna-rada-posylyla-vidpovidalnosti-za-zlochyny-proty-zhurnalistiv/

5. *Вступ до безпеки* [Електронний ресурс] : онлайн-курс з громадянської журналістики. – Електрон. текст. дані. – Режим доступу: https://school-cj.org/courses/security

6. *Гарантії забезпечення свободи слова* [Електронний ресурс] : інформація підготовлена з використанням Звіту Генерального Секретаря РЄ Турбйорна Ягланда «Демократично-правова держава, права людини та верховенство права. Популізм –

особливості системи стримувань і противаг у Європі». – Електрон. текст. дані. – Режим доступу: https://www.nrada.gov.ua/foreign_practice/

7. *«Гендер в деталях» випустив серію жартівливих картинок для журналістів на тему сексизму* [Електронний ресурс] / Ін-т мас. інформації. – Електрон. текст. дані. – Режим доступу: http://imi.org.ua/news/hender-v-detalyah-vypustyv-seriyu-zhartivlyvyh-kartynok-dlya-zhurnalistiv-na-temu-seksyzmu/

8. *Довідник безпеки журналістів* [Електронний ресурс] / Центр журналіст. солідарності. – Електрон. текст. дані. – Режим доступу: http://www.cje.org.ua/sites/default/files/library/Dovydnik-bezpeki-gurnalistiv.pdf

9. Земляна І., Романюк О. *Журналіст і (НЕ)безпека. Посібник для журналістів, які працюють в небезпечних умовах* [Електронний ресурс] / І. Земляна, О. Романюк. – Електрон. текст. дані. – Режим доступу: http://imi.org.ua/wp-content/uploads/2017/06/Zhurnalist-i-nebezpeka.pdf

10. Зубченко Я. Я. *Погляд у майбутнє. Чого досягли окуляри доповненої реальності* [Електронний ресурс] / Я. Зубченко // MediaSapiens. – Електрон. текст. дані. – Режим доступу: https://ms.detector.media/trendi/post/26194/2020-12-15-poglyad-u-maybutnie-chogo-dosyagly-okulyary-dopovnenoi-realnosti/

11. *Інститут масової інформації створив сайт з безпеки для журналістів* [Електронний ресурс] / Детектор медіа. – Електрон. текст. дані. – Режим доступу: http://detector.media/infospace/article/118301/2016-08-

31-institut-masovoi-informatsii-stvoriv-sait-z-bezpeki-dlya-zhurnalistiv/

12. *Інформаційна безпека: соціально-правові аспекти* [Електронний ресурс] : підручник / Б. В. Остроухов [та ін.] ; за заг. ред. Є. Д. Скулиша. – Київ : КНТ, 2011. – 776 с. – Електрон. текст. дані. – Режим доступу: http://www.dut.edu.ua/uploads/l_1352_84114000.pdf

13. Кастельс М. *Інтернет-Галактика*. – Київ : Ваклер, 2007. – 290 с.

14. *Категорія: цифрова безпека* [Електронний ресурс] / Центр журналіст. солідарності. – Електрон. текст. дані. – Режим доступу: http://j-sos.org.ua/category/novyny/tsyfrova-bezpeka/

Інформаційні ресурси

1. Цифрова безпека журналістів та інших працівників медіа. Prometheus. URL: https://courses.prometheus.org.ua/courses/coursev1:Prometheus+DSJ101+2022_T1/about (дата звернення: 15.03.2025).

2. Суспільне мовлення. URL: https://suspilne.media/ (дата звернення: 15.03.2025).

3. Умови та правила Facebook. URL: https://ru-ru.facebook.com/policies (дата звернення: 15.03.2025).

4. Організація Об'єднаних націй. URL: https://www.un.org/ru/ (дата звернення: 15.03.2025).

5. Європейський суд з прав людини. URL: https://www.echr.coe.int/Pages/home.aspx?p=applicants/ukr&c (дата звернення: 15.03.2025).

6. Справи Європейського суду з прав людини. URL: https://hudoc.echr.coe.int/rus (дата звернення: 15.03.2025).

7. Міністерство інформаційної політики України. URL: https://mip.gov.ua/ (дата звернення: 15.03.2025).
8. Центр демократії та верховенства права. URL: https://cedem.org.ua/ (дата звернення: 15.03.2025).
9. Харківська правозахисна група. URL: http://khpg.org/ (дата звернення: 15.03.2025).
10. Незалежна медійна рада. URL: www.mediarada.org (дата звернення: 15.03.2025).