МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Ю. П. Синиціна

ОСНОВИ КІБЕРГІГІЄНИ

Методичні рекомендації
для підготовки до практичних занять

для здобувачів першого (бакалаврського) рівня вищої освіти
зі спеціальності F3 «Комп'ютерні науки»

Дніпро
2026

УДК 004.056
С 38

Схвалено Науково-методичною радою Дніпровського державного університету внутрішніх справ (протокол № 9 від 20.05.2026)

РЕЦЕНЗЕНТИ:

Микола ОСИПЧУК, доцент кафедри фізики та прикладної математики Український державний університет науки і технологій

Ольга СТАНІНА, доцент кафедри системного аналізу та управління Національного технічного університету «Дніпровська політехніка»

УКЛАДАЧ:

Юлія СИНИЦІНА, доцент кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат технічних наук, доцент.

С 38 Синиціна Ю. П. Основи кібергігієни : метод. реком. для підгот. до практ. занять (для здоб. перш. (бакалаврського) рівня вищ. освіти зі спец. F3 «Комп'ютерні науки»). Дніпро: ДДУВС, 2026. 56 с.

Методичні рекомендації для підготовки до практичних занять з тем, передбачених навчальним планом з дисципліни «Основи кібергігієни».

Для здобувачів першого рівня вищої освіти зі спеціальності F3 «Комп'ютерні науки» заочної форми навчання та викладачів закладів вищої освіти.

ЗМІСТ

ВСТУП

У сучасному стеку технологій, де розробка програмного забезпечення, архітектура баз даних та алгоритми штучного інтелекту стають основою функціонування суспільства, безпека коду та систем починається з безпеки самого розробника. Для майбутнього фахівця з комп'ютерних наук кібергігієна – це не просто набір користувацьких правил, а професійний фундамент. Це дисципліна, що вивчає методи мінімізації цифрових ризиків на рівні персональної взаємодії з інформаційними системами, що є критично важливим для створення стійких та надійних ІТ-продуктів у майбутньому.

Цифрові інструменти сьогодні дозволяють автоматизувати аналітичну роботу та обробляти великі масиви даних, проте кожна інтеграція чи розгортання середовища (deployment) створює нові вектори атак. Розуміння закономірностей у виявленні вразливостей та моделювання сценаріїв загроз є необхідною умовою для формування обґрунтованих технічних рішень. Використання принципів кібергігієни підвищує точність проектування та оперативність реагування на інциденти, що є обов'язковою компетенцією для фахівця рівня Bachelor of Computer Science.

Метою вивчення навчальної дисципліни «Основи кібергігієни» є формування у здобувачів вищої освіти цілісного уявлення про принципи, методи та інструменти забезпечення особистої та корпоративної безпеки в кіберпросторі. Дисципліна покликана ознайомити з основними кіберзагрозами та їхніми наслідками, а також навчити розпізнавати їх і протидіяти.

Очікувані результати навчання:

знати:

– основні поняття кібергігієни, інформаційної безпеки та захисту персональних даних;

– основні кіберзагрози (шкідливе ПЗ, фішинг, соціальна інженерія, кібершахрайство) та методи їх запобігання;

– принципи безпечної роботи в мережі Інтернет та використання цифрових сервісів;

– основи політик безпеки в організаціях та законодавчі аспекти захисту інформації;

– правила створення та використання надійних паролів і двофакторної аутентифікації;

– основи етичного використання інформаційних технологій та принципи цифрової культури.

вміти:

– оцінювати рівень власної кібергігієни та визначати потенційні ризики у цифровому середовищі;

– застосовувати базові заходи захисту інформації (антивірусні програми, шифрування, резервне копіювання);

– користуватися інструментами безпечного доступу до ресурсів Інтернету та хмарних сервісів;

– ідентифікувати та реагувати на потенційні кібератаки та підозрілі дії у мережі;

– дотримуватися правил безпечного обміну інформацією та цифрової етики у навчальній і професійній діяльності;

– аналізувати сучасні тенденції у сфері кібербезпеки та пропонувати заходи щодо підвищення кібергігієни у колективних проєктах.

– Вивчення дисципліни забезпечує формування компетентностей за освітньою програмою: Комп'ютерні науки.

Інтегральна компетентність – здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК1 – Здатність до абстрактного мислення, аналізу та синтезу.

ЗК3 – Знання та розуміння предметної області та розуміння професійної діяльності.

Спеціальні компетентності:

СК14 – Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

СК17 – Здатність забезпечувати безпеку інформаційних систем та мереж, розробляти та впроваджувати засоби захисту інформації, аналізувати та управляти ризиками в інформаційній безпеці.

СК18 – Володіння сучасними методами захисту інформації, розуміння принципів роботи алгоритмів шифрування, блокчейн-технологій та їх застосування у комп'ютерних системах.

Пререквізити та постреквізити дисципліни:

Пререквізити: базові знання після закінчення закладів середньої освіти.

Постреквізити: «Операційні системи та їх адміністрування», «Комп'ютерні мережі та їх безпека», «Технології комп'ютерного проєктування та об'єктно-орієнтоване програмування». «Адміністрування та організація сучасних обчислювальних систем», «Інформаційні системи та

технології. Технології захисту даних», «Бази даних та технології захисту баз даних»

Здобувачі вищої освіти повинні продемонструвати такі **результати навчання**:

РН16 – Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

РН18 – Здатність проєктувати та впроваджувати безпечні інформаційні системи; проектувати архітектуру інформаційних систем з урахуванням вимог захисту конфіденційної інформації.

РН19 – Здатність ідентифікувати, оцінювати та запобігати загрозам інформаційної безпеки та розробляти ефективні заходи протидії, використовуючи сучасні інструменти та методики інформаційної безпеки.

ТЕМА 1. ВСТУП ДО КІБЕРГІГІЄНИ ТА ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Зміст теми:

Поняття кібергігієни та її значення для сучасного користувача. Основні кіберзагрози та їх класифікація. Принципи безпечного використання персональних пристроїв і мережі Інтернет.

Практичне заняття № 1 – 2 год.

Мета: сформувати вміння оцінювати власний рівень кібергігієни. Навчитися перевіряти надійність паролів, налаштовувати параметри безпеки браузера та електронної пошти. Розробити індивідуальний план кібергігієни для щоденного використання.

План:

1. Поняття кібергігієни та її значення для сучасного користувача.
2. Основні кіберзагрози та їх класифікація.
3. Принципи безпечного використання персональних пристроїв і мережі Інтернет.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *кібергігієна, кіберзагроза, шкідливе програмне забезпечення, соціальна інженерія, фішинг, несанкціонований доступ, DDoS-атака, аутентифікація двофакторна аутентифікація (2FA), VPN (Virtual Private Network).*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Поняття кібергігієни та її значення для сучасного користувача

Кібергігієна – це сукупність правил, навичок та практик безпечної поведінки користувача у цифровому середовищі, спрямованих на захист персональних даних, пристроїв і цифрових ресурсів.

Подібно до звичайної гігієни, вона є профілактичним інструментом, що зменшує ризик потрапляння під дію шкідливих програм, шахрайських схем чи витоку даних.

Значення для користувача:

- захист персональної інформації від зловмисників;
- збереження працездатності пристроїв;
- підвищення рівня довіри у цифрових сервісах;
- формування цифрової культури та відповідальності.

2. Основні кіберзагрози та їх класифікація

Кіберзагрози – це дії чи події, які можуть призвести до втрати конфіденційності, цілісності або доступності інформації.

Класифікація кіберзагроз:

1. *Шкідливе програмне забезпечення (Malware):* віруси, трояни, шпигунські програми, програми-вимагачі.
2. *Соціальна інженерія:* фішинг, підроблені сайти, шахрайські листи, телефонні дзвінки від шахраїв.
3. *Несанкціонований доступ:* злам акаунтів, підбір паролів, використання вразливостей у системах.
4. *Мережеві атаки:* DDoS-атаки, перехоплення даних у відкритих Wi-Fi мережах.
5. *Витоки інформації:* оприлюднення персональних даних через зламані сервіси або необережні дії користувача.

3. Принципи безпечного використання персональних пристроїв і мережі Інтернет

1. Надійні паролі та автентифікація
2. Використання складних паролів (не менше 12 символів, поєднання літер, цифр та символів).
3. Використання менеджерів паролів.
4. Обов'язкове застосування двофакторної аутентифікації (2FA).
5. Оновлення та захист пристроїв
6. Регулярне оновлення операційної системи та програмного забезпечення.
7. Використання антивірусів і фаєрволів.
8. Уникання завантаження програм із неперевірених джерел.
9. Безпека в Інтернеті
10. Перевірка достовірності сайтів (HTTPS, правильність адреси).
11. Обережність із вкладеннями у пошті.
12. Уникання використання відкритих Wi-Fi без VPN.
13. Керування персональними даними
14. Мінімізація публікації особистої інформації у соцмережах.
15. Перевірка налаштувань приватності у сервісах.
16. Використання окремих поштових адрес для роботи, особистого життя та реєстрацій на сайтах.

Таким чином, кібергігієна є базовою компетентністю сучасної людини, яка дозволяє знизити ризики цифрових загроз та забезпечити особисту інформаційну безпеку.

Завдання:

Завдання 1. Перевірка надійності паролів (надати скріни для підтвердження):

1. Проаналізувати власні паролі (без розкриття викладачу).
2. Перевірити їхню стійкість за допомогою онлайн-сервісів (наприклад, https://howsecureismypassword.net, https://haveibeenpwned.com).
3. Скласти правила створення надійних паролів.

Завдання 2. Налаштування безпеки браузера (надати скріни для підтвердження):

1. Увімкнути блокування небезпечних сайтів і завантажень.
2. Перевірити, чи активовано автоматичне оновлення браузера.
3. Очистити кеш та налаштувати автоматичне видалення cookie-файлів.

Завдання 3. Налаштування безпеки електронної пошти:

1. Увімкнути двофакторну аутентифікацію.
2. Перевірити налаштування відновлення доступу.
3. Ознайомитися з прикладами фішингових листів і навчитися розпізнавати їх.

Завдання 4. Складання персонального «Плану кібергігієни». Приклад фрагменту плану у додатку 1:

1. Визначити щоденні дії для підтримання безпеки (оновлення, перевірка пошти, резервне копіювання).
2. Визначити щотижневі дії (перевірка пристроїв на віруси, моніторинг налаштувань безпеки).

Завдання 5. Авторизуватись на сайті chat.openai.com. «Напиши якісний Google dork для пошуку моїх персональних даних в мережі Інтернет. Мене звати…». Сформуй власний «Чеклист OSINT-перевірки себе»

Завдання 6: Пройти тест за темою.

Вимоги до оформлення практичної роботи

Тема: Огляд та тестування AI-сервісів для юристів

Мета: ознайомитися з сучасними AI-інструментами для правового пошуку, протестувати їхню ефективність та порівняти з традиційними базами даних.

1. Загальні вимоги

Робота виконується у текстовому редакторі MS Word / Google Docs. У електронному вигляді (формати .docx, для використання у системах СУДН «Moodle»).

Обсяг – 8-12 сторінок друкованого тексту.

Формат сторінки: А4, поля: верхнє – 20 мм, нижнє – 20 мм, ліве – 25 мм, праве – 15 мм. Шрифт: Times New Roman, розмір – 14 пт.

Інтервал – 1,5. Абзацний відступ – 1,25 см. Нумерація сторінок – з правого нижнього кута.

Усі таблиці, рисунки, схеми повинні мати назву та номер.

Використані джерела подаються у списку літератури за ДСТУ 8302:2015.

2. Структура роботи

Титульний аркуш (назва міністерству, назва закладу, дисципліна, тема, дані здобувача вищої освіти і викладача, рік).

Мета та завдання роботи.

Хід виконання роботи:

Крок 1. Вибір інструментів (з поясненням). Крок 2. Формування правового запиту.

Крок 3. Робота з AI-сервісами (результати кожного інструменту). *Крок 4.* Робота з традиційною базою даних (аналіз ЄДРСР).

Крок 5. Порівняльний аналіз (таблиця + коментарі).

Висновки (3–5 узагальнених тез про результати роботи).

Список використаних джерел (не менше 5, у т.ч. нормативні акти).

Додатки (за наявності: скріншоти роботи з сервісами, фрагменти результатів пошуку).

Контрольні питання

1. Дайте визначення штучного інтелекту та назвіть основні напрями його застосування у праві.
2. Які AI-інструменти використовуються для автоматизації юридичних досліджень?
3. У чому полягає принцип роботи системи прогнозування судових рішень?
4. Які фактори можуть впливати на точність прогнозів AI у судових справах?
5. Назвіть приклади міжнародних ініціатив зі стандартизації етичного використання AI у праві.
6. Які основні юридичні ризики пов’язані з використанням AI у правозастосуванні практиці?
7. Що таке алгоритмічна упередженість та як вона може впливати на судові рішення?
8. Як AI може підвищити ефективність роботи адвокатів та юристів?
9. Чим відрізняється правовий статус рішень, ухвалених AI, від рішень людини?
10. Які етичні виклики постають при впровадженні AI у правову сферу?

Список використаних джерел до теми 1

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 24.04.2026).

2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 24.04.2026).

3. ЮНЕСКО. Recommendation on the Ethics of Artificial Intelligence [Електронний ресурс]. URL : https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence (дата звернення 24.04.2026).

4. Кабінет Міністрів України. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження від 02.12.2020 № 1556-р [Електронний ресурс]. База даних «Законодавство України» / Верховна Рада

України. URL : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення 24.04.2026).

5. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с. URI: https://er.dduvs.edu.ua/handle/123456789/7110 (дата звернення 24.04.2026);

6. Інформаційні та комунікаційні технології : навч. посіб. / О. А. Дісковський, Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов. Дніпро: Дніпров. держ. ун-т внутр. справ, 2025. 272 с. URL : https://er.dduvs.edu.ua/handle/123456789/16603 (дата звернення 24.04.2026).

7. Синиціна Ю. П., Дудник В. В. Актуальні питання взаємозв'язку інформаційної та національної безпеки України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро: ДДУВС, 2020. с. 164-167 URL : https://er.dduvs.edu.ua/bitstream/123456789/5920/1/44.pdf (дата звернення: 24.04.2026).

8. Синиціна Ю. П. Інформаційна безпека в умовах воєнного стану / Ю. П. Синиціна // Сучасні пріоритети розвитку України: економічна та інформаційна безпека : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 10 жовтня 2023 р.). Дніпро : ДДУВС, 2024. С. 40-42. URL : https://er.dduvs.edu.ua/handle/123456789/15030 (дата звернення: 24.04.2026).

ТЕМА 2. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЦИФРОВИХ ОБЛІКОВИХ ЗАПИСІВ

Зміст теми:

Основи створення надійних паролів та двофакторної аутентифікації. Політика приватності в соціальних мережах та хмарних сервісах. Шифрування даних та безпечне зберігання інформації.

Практичне заняття № 2 – 2 год.

Мета: сформувати практичні навички створення надійних паролів і перевірки їхньої стійкості; навчитися налаштовувати двофакторну аутентифікацію (2FA) у різних онлайн-сервісах; ознайомитися з принципами шифрування даних та відпрацювати практику їх застосування.

План:

1. Основи створення надійних паролів та двофакторної аутентифікації;
2. Політика приватності в соціальних мережах та хмарних сервісах;
3. Шифрування даних та безпечне зберігання інформації.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *пароль, надійний пароль, двофакторна аутентифікація (2FA), шифрування, дешифрування, політика приватності, обліковий запис (акаунт), менеджер паролів, резервне копіювання (backup), фішинг.*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Основи створення надійних паролів та двофакторної аутентифікації (2FA)

Надійні паролі:

Пароль має бути не менше 12 символів і містити комбінацію великих і малих літер, цифр та спеціальних символів.

Уникати очевидних комбінацій, таких як дати народження, імена, прості слова («password», «123456»).

Використовувати менеджери паролів для генерації та зберігання складних паролів.

Двофакторна аутентифікація (2FA), *приклади увімкнення двофакторної аутентифікація (2FA) у сервісах: Google, Facebook наведено у додатку 2:*

2FA додає додатковий рівень захисту: крім пароля потрібно ввести код із SMS, електронної пошти або спеціального додатку (Google Authenticator, Authy).

Навіть у випадку компрометації пароля зловмисник не зможе отримати доступ без другого фактору.

Рекомендується включати 2FA для електронної пошти, соціальних мереж, хмарних сервісів та онлайн-банкінгу.

2. Політика приватності в соціальних мережах та хмарних сервісах

Основні принципи:

Перевіряти налаштування приватності облікового запису, обмежуючи доступ до особистих даних.

Мінімізувати публікацію персональної інформації у відкритому доступі (дата народження, адреса, телефони, документи).

Розділяти акаунти для роботи, особистого життя та реєстрацій на сторонніх сайтах.

Читати та розуміти умови використання сервісів і політику обробки персональних даних.

Використовувати надійні хмарні сервіси з підтримкою шифрування та захисту даних.

Ризики при порушенні політики приватності:

Викрадення особистих даних та акаунтів.

Цілеспрямовані атаки фішингу та соціальної інженерії.

Потрапляння особистої інформації у відкритий доступ без вашого дозволу.

3. Шифрування даних та безпечне зберігання інформації

Шифрування:

Процес перетворення даних у незрозумілу для сторонніх форму за допомогою спеціальних алгоритмів.

Існує симетричне шифрування (один ключ для шифрування і дешифрування) та асиметричне (публічний і приватний ключі).

Шифрування забезпечує конфіденційність даних, навіть якщо файли потраплять до третіх осіб.

Безпечне зберігання даних:

Використання надійних носіїв та хмарних сервісів із шифруванням та резервним копіюванням.

Встановлення антивірусного ПЗ та брандмауера для захисту від шкідливих програм.

Розмежування даних: особисті, робочі, тимчасові файли.

Використання паролів та доступів за ролями для спільних ресурсів.

Рекомендації:

Завжди шифрувати важливі файли перед передачею або зберіганням у хмарі.

Регулярно оновлювати програмне забезпечення та перевіряти цілісність файлів.

Використовувати окремі облікові записи для роботи з конфіденційною інформацією.

Якщо бажаєте, я можу написати до цього тексту практичні завдання та приклад виконання у форматі для студентів.

Завдання:

Завдання 1: Створення та тестування надійних паролів.

1. Створіть 2–3 паролі, що відповідають сучасним вимогам (12+ символів, великі та малі літери, цифри, спецсимволи).
2. Перевірте їхню стійкість за допомогою онлайн-сервісу або спеціальної програми.

Завдання 2: Налаштування двофакторної аутентифікації (2FA)

1. Увімкніть 2FA у вибраному сервісі (Google, Facebook, GitHub, Microsoft тощо). Приклади увімкнення знаходяться в додатках.
2. Підтвердження тимчасовим кодом.
3. Продемонструйте процес входу із застосуванням 2FA (скріншот кроків або код із додатку).
4. Перевірка та налаштування політики приватності
5. Перевірте налаштування приватності свого акаунту у соцмережах або хмарних сервісах.
6. Встановіть обмеження на публічний доступ до персональних даних.
7. Використайте окрему електронну адресу для реєстрацій на сторонніх сайтах.

Завдання 3: Шифрування та дешифрування файлів

1. Створіть текстовий файл із тестовою інформацією (наприклад, контактні дані).
2. Використайте доступне програмне забезпечення (7-Zip, VeraCrypt, GnuPG) для шифрування файлу.
3. Перевірте правильність дешифрування.
4. Висновки.
5. Опишіть ефективність створених паролів та 2FA.

Завдання 4: Пройти тест за темою

Вимоги до оформлення кейсів
ТЕМА: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ
ТА ЦИФРОВИХ ОБЛІКОВИХ ЗАПИСІВ.

Мета: сформувати практичні навички створення надійних паролів і перевірки їхньої стійкості; навчитися налаштовувати двофакторну аутентифікацію (2FA) у різних онлайн-сервісах; ознайомитися з принципами шифрування даних та відпрацювати практику їх застосування..

Загальні вимоги:

Робота виконується українською мовою.

Текст оформлюється у текстовому редакторі (MS Word, Google Docs або інший сумісний).

Формат сторінки: А4, шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5.

Поля: верхнє та нижнє – 20 мм, ліве – 25 мм, праве – 15 мм.

Нумерація сторінок – у правому верхньому куті, починаючи з другої сторінки.

Структура роботи:

Титульний аркуш (назва міністерства, назва навчального закладу, дисципліна, тема роботи, ПІБ студента, група, дата, ПІБ викладача).

Мета роботи – коротко, що студент повинен засвоїти.

Хід виконання завдань – опис дій здобувача відповідно до методичних вказівок.

Скріншоти із налаштуваннями чи результатами виконання.

Висновки – 5–7 речень про отримані результати.

Додатки – таблиці, схеми, інструкції (за наявності).

Оформлення ілюстрацій та таблиць

Скріншоти мають бути зрозумілими, з підписами та нумерацією (наприклад: Рис. 1. Перевірка надійності пароля).

Таблиці нумеруються і мають заголовки (Таблиця 1. План кібергігієни).

Формат зображень: вставляти без спотворень, бажано у центрі сторінки.

Обсяг роботи:

Мінімальний – 3–5 сторінок основного тексту без урахування титульного аркуша та додатків.

Максимальний – 10–12 сторінок.

Контрольні питання

1. Що таке надійний пароль і які правила його створення?
2. Навіщо потрібна двофакторна аутентифікація (2FA)?
3. Назвіть види двофакторної аутентифікації.
4. Які основні загрози існують у соціальних мережах щодо персональних даних?
5. Що таке політика приватності у хмарних сервісах?
6. Наведіть приклади методів шифрування даних.
7. Як безпечно зберігати інформацію на персональному пристрої та у хмарі?

Список використаних джерел до теми 2

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.04.2026).

2. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.04.2026).

3. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR) [Електронний ресурс]. URL : https://gdprinfo.eu/ (дата звернення 24.04.2026);

4. Європейська конвенція про захист прав людини і основоположних свобод Рада Європи. Європейська конвенція про захист прав людини і основоположних свобод (European Convention on Human Rights) [Електронний ресурс]. URL : https://www.echr.coe.int/d/convention_ukr (дата звернення 24.04.2026);

5. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с. URL : https://er.dduvs.edu.ua/handle/123456789/7110 (дата звернення 24.04.2026);

6. Інформаційні та комунікаційні технології : навч. посіб. / О. А. Дісковський, Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов. Дніпро: Дніпров. держ. ун-т внутр. справ, 2025. 272 с. URL : https://er.dduvs.edu.ua/handle/123456789/16603 (дата звернення 24.04.2026).

7. Синиціна Ю. П., Станіна О. Д. Обґрунтування актуальності цифрової комунікація закладів вищої освіти (Rationale for the relevance of digital communication in higher education institutions) Міжн. колект.моногр. / Selected aspects of digital society development «Digital Economyand Digital Society» III Міжнародна конференція (28-29 травня 2021 р.) Katowice, University of Technology, Poland, 2021.mon # 45. 148- 156 с., URL : http://www.wydawnictwo.wst.pl/uploads/files/337190b4d66761009188e7904791336d.pdf (дата звернення: 24.04.2026).

8. Синиціна Ю. П. Сучасні підходи до безпеки операційних систем Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро: ДДУВС, 2020. с. 66-68; URL : https://er.dduvs.edu.ua/bitstream/123456789/5964/1/8.pdf (дата звернення: 24.04.2026).

ТЕМА 3. КІБЕРЗАГРОЗИ ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ

Зміст теми:

Види шкідливого ПЗ (віруси, трояни, шпигунські програми). Фішинг, соціальна інженерія та шахрайство в Інтернеті. Антивірусний захист та принципи оновлення програмного забезпечення.

Практичне заняття № 3 – 2 год.

Мета: сформувати практичні навички виявлення кіберзагроз, розпізнавання фішингових атак та застосування антивірусного захисту.

План:

1. Види шкідливого ПЗ (віруси, трояни, шпигунські програми).
2. Фішинг, соціальна інженерія та шахрайство в Інтернеті.
3. Антивірусний захист та принципи оновлення програмного забезпечення.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *вірус, троян (Trojan horse), Spyware (шпигунське ПЗ), Ransomware (програма-вимагач), фішинг, DDoS-атака, брандмауер (фаєрвол), антивірус, оновлення програмного забезпечення (патчі)*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Види шкідливого програмного забезпечення (ПЗ)

Шкідливе програмне забезпечення (malware) – це програми або коди, створені з метою завдати шкоди комп’ютеру, мережі чи користувачеві. Основні види:

Віруси – програми, що проникають у файли та системи, поширюються через носії, електронну пошту чи інтернет. Можуть видаляти, пошкоджувати або викрадати дані.

Трояни (Trojan horses) – шкідливі програми, що маскуються під корисне ПЗ. Дають зловмисникам доступ до пристрою користувача.

Шпигунські програми (Spyware) – ПЗ, що непомітно збирає інформацію про дії користувача: паролі, дані банківських карток, історію перегляду тощо.

Фішинг, соціальна інженерія та шахрайство в Інтернеті

Фішинг – отримання конфіденційної інформації шляхом маскування під довірені сервіси (листи від «банку», «державних органів», «служб доставки»). Мета – викрадення паролів, фінансових даних.

Соціальна інженерія – маніпулювання людиною для отримання інформації чи доступу (дзвінки від «служби підтримки», прохання надати код підтвердження).

Шахрайство в Інтернеті – підроблені інтернет-магазини, фальшиві інвестиційні проекти, схеми швидкого збагачення.

2. Антивірусний захист

Антивірус – це програмне забезпечення, що виявляє, блокує та видаляє шкідливі програми. Основні принципи його використання:

- регулярне оновлення антивірусних баз;
- сканування файлів та системи;
- контроль завантажень і електронної пошти;
- використання брандмауера (фаєрволу) для захисту мережевого трафіку.

Принципи оновлення програмного забезпечення

Своєчасне оновлення операційної системи та додатків закриває відомі вразливості.

Використання офіційних джерел оновлень гарантує безпеку.

Автоматичне оновлення зменшує ризик забути про встановлення важливих «латок безпеки».

Кіберзагрози є багатогранними і постійно розвиваються, але більшість із них можна попередити завдяки базовим навичкам кібергігієни: використанню антивірусу, своєчасному оновленню програмного забезпечення, уважності до повідомлень та критичному ставленню до онлайн-комунікацій.

Завдання:

Завдання 1: Аналіз підозрілого листа (фішинг):

1. Знайти зразок фішингового листа (навчальний приклад).
2. Визначити ознаки шахрайства: підозріла адреса відправника, помилки у тексті, підроблений логотип, посилання на сторонній сайт.
3. Зробити висновок: чому цей лист небезпечний.

Завдання 2: Перевірка файлів на віруси:

1. *Завантажити файл-приклад (навчальний, безпечний).*
2. *Використати сервіс VirusTotal*
3. *або встановлений антивірус.*
4. *Зробити скріншот результатів перевірки.*

Завдання 3: Налаштування антивірусного захисту:

1. Відкрити меню встановленого антивірусного програмного забезпечення.
2. Перевірити: чи активне автоматичне оновлення, чи увімкнено захист у реальному часі.
3. За потреби – внести зміни.

Завдання 4: Оновлення програмного забезпечення:

1. *Перевірити доступні оновлення для операційної системи.*
2. *Зробити скріншот перед оновленням.*
3. *Встановити оновлення та повторно зафіксувати результат.*

Завдання 5: Пройти тест за темою

Приклад виконання наведено у додатку 3.

Вимоги до оформлення практичної роботи

Тема: ТЕМА 3. КІБЕРЗАГРОЗИ ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ.

Мета: сформувати практичні навички виявлення кіберзагроз, розпізнавання фішингових атак та застосування антивірусного захисту.

Загальні вимоги

Робота виконується українською мовою.

Текст оформлюється у текстовому редакторі (MS Word, Google Docs або інший сумісний).

Формат сторінки: А4, шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5.

Поля: верхнє та нижнє – 20 мм, ліве – 25 мм, праве – 15 мм.

Нумерація сторінок – у правому верхньому куті, починаючи з другої сторінки.

Структура роботи

Титульний аркуш (назва міністерства, назва навчального закладу, дисципліна, тема роботи, ПІБ студента, група, дата, ПІБ викладача).

Мета роботи – коротко, що студент повинен засвоїти.

Хід виконання завдань – опис дій здобувача відповідно до методичних вказівок.

Скріншоти із налаштуваннями чи результатами виконання.

Висновки – 5–7 речень про отримані результати.

Додатки – таблиці, схеми, інструкції (за наявності).

Оформлення ілюстрацій та таблиць

Скріншоти мають бути зрозумілими, з підписами та нумерацією (наприклад: Рис. 1. Перевірка надійності пароля).

Таблиці нумеруються і мають заголовки (Таблиця 1. План кібергігієни).

Формат зображень: вставляти без спотворень, бажано у центрі сторінки.

Обсяг роботи

Мінімальний – 3–5 сторінок основного тексту без урахування титульного аркуша та додатків.

Максимальний – 10–12 сторінок.

Контрольні питання

1. Назвіть основні види шкідливого програмного забезпечення.
2. В чому відмінність вірусу, трояна і шпигунської програми?
3. Що таке фішинг і як його розпізнати?
4. Поясніть поняття «соціальна інженерія» та наведіть приклади.
5. Які основні принципи антивірусного захисту?
6. Чому важливо регулярно оновлювати програмне забезпечення?
7. Назвіть приклади безпечної поведінки у мережі для запобігання кібератакам.
8. Як можна перевірити, що файл чи посилання безпечні перед відкриттям?

Список використаних джерел до теми 3

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних система: Постанова КМУ від 8 лютого 2021 року № 92. URL : https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text (дата звернення 24.04.2026).
2. ISO/IEC 27043:2015. Information technology. Security techniques. Incident investigation principles and processes [Електронний ресурс]. ISO/IEC. URL: https://webstore.iec.ch/en/publication/24354 (дата звернення 24.04.2026).
3. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 181 с. URL : https://er.dduvs.edu.ua/handle/123456789/15045 (дата звернення 24.04.2026).
4. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с. URL : https://er.dduvs.edu.ua/handle/123456789/7110 (дата звернення 24.04.2026);
5. Інформаційні та комунікаційні технології : навч. посіб. / О. А. Дісковський, Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов. Дніпро: Дніпров. держ. ун-т внутр. справ, 2025. 272 с. URL : https://er.dduvs.edu.ua/handle/123456789/16603 (дата звернення 24.04.2026).
6. Синиціна Ю. П. APT-атак – пріоритетний напрямок розвитку кібербезпеки Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф. 19.12. 2020 р., м. Львів : ЛьвДУВС, 2020. с. 66-68. URL : https://www2.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/19_12_2020.pdf (дата звернення: 24.04.2026).

7. Синиціна Ю. П., Кліменко А. О. Актуальні питання інформаційної безпеки в діяльності Національної поліції України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро: ДДУВС, 2020. с. 174-176. URL : https://er.dduvs.edu.ua/bitstream/123456789/5918/1/46.pdf (дата звернення: 24.04.2026).

8. Офіційний сайт Національної поліції України: URL : https://www.npu.gov.ua/.

ТЕМА 4. ПОШУК ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ. ОСОБИСТА БЕЗПЕКА В ІНТЕРНЕТІ

Зміст теми:

Історія розвитку та загальна характеристика пошукових систем. Пошук інформації за допомогою GOOGLE: сервіси, спеціальний пошук, апаратне забезпечення та інструменти. Мета-пошукові системи та системи анонімного пошуку інформації. Пошук оперативної інформації в соціальних мережах Facebook. Застосування чат-ботів у месенджері Telegram. Особиста безпека у інтернеті.

Практичне заняття № 4 – 2 год.

Мета: ознайомитися з історією розвитку пошукових систем. Навчитися використовувати базові та розширені можливості Google для пошуку інформації. Опрацювати навички роботи з мета-пошуковими системами та системами анонімного пошуку. Розвинути практичні вміння перевірки достовірності та релевантності знайденої інформації.

План:

1. Історія розвитку та загальна характеристика пошукових систем
2. Пошук інформації за допомогою GOOGLE: сервіси, спеціальний пошук, апаратне забезпечення та інструменти
3. Мета-пошукові системи та системи анонімного пошуку інформації
4. Базові поняття та методи соціальної інженерії: фішингові імейли, сайти та заражене програмне забезпечення
5. Безпека в інтернеті: онлайн-репутація, шкідливий онлайн-контент, секстинг, сексторшен, кіберсталкінг».
6. Безпека в інтернеті: кібербулінг, кібергрумінг, тролінг, флеймінг, хепіслепінг, хейтспіч, доксинг, кетфішинг.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *OSINT (Open Source Intelligence), метапошукова система, соціальна інженерія, цифровий слід, пошукові системи, анонімізація, спеціалізований пошук, фішинг, кібергігієна, достовірність джерела.*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Історія розвитку та загальна характеристика пошукових систем

Пошукові системи з’явилися як відповідь на зростання обсягів інформації в мережі Інтернет. Перші пошукові каталоги з’явилися у 1990-х роках і мали вигляд списків сайтів, які вручну додавали адміністратори (наприклад, Yahoo Directory). Згодом виникла потреба в автоматизованих системах, здатних швидко індексувати та знаходити дані.

У 1993 році з’явився Archie, який вважають першим інструментом пошуку файлів у мережі. Пізніше з’явилися AltaVista, Lycos, Excite, які впровадили алгоритми індексації та пошуку за ключовими словами. Справжній прорив зробила компанія Google у 1998 році, запропонувавши алгоритм PageRank, що визначав важливість сторінки на основі кількості та якості посилань.

Сучасні пошукові системи – це складні програмно-апаратні комплекси, що використовують штучний інтелект, машинне навчання та великі бази даних для швидкого доступу до потрібної інформації. Вони дозволяють працювати з мультимедіа, картами, науковими статтями, новинами та іншими ресурсами.

2. Пошук інформації за допомогою GOOGLE: сервіси, спеціальний пошук, апаратне забезпечення та інструменти

Google є найпопулярнішою пошуковою системою у світі. Вона надає широкий набір сервісів для різних цілей:

Google Search – основний пошук за ключовими словами та фразами.

Google Scholar – спеціалізований пошук наукових публікацій.

Google Books – пошук книг і журналів.

Google News – агрегатор новин.

Google Images – пошук зображень, включно з інструментами зворотного пошуку.

Google Maps та Google Earth – пошук географічних даних, карт і навігації.

Google Patents – пошук патентів.

Google Trends – аналіз популярності запитів.

Для роботи зі спеціальними запитами існують оператори пошуку:

"" – точна фраза,

site: – пошук на конкретному сайті,

filetype: – пошук файлів певного формату,

intitle: – пошук у заголовках сторінок.

Google використовує величезні дата-центри, потужні сервери, алгоритми штучного інтелекту та системи кешування для обробки мільярдів запитів щодня.

3. Мета-пошукові системи та системи анонімного пошуку інформації

Окрім класичних пошуковиків, існують мета-пошукові системи, які одночасно надсилають запити до кількох пошукових систем і агрегують результати. Приклади: Dogpile, Metacrawler, Startpage. Вони дозволяють отримати більш широкий спектр результатів без обмеження одним джерелом.

Системи анонімного пошуку забезпечують конфіденційність користувача. Вони не зберігають історію пошуку та не відслідковують IP-адресу. Найвідоміші приклади:

DuckDuckGo – не відстежує користувачів і не персоналізує результати.

Startpage – використовує результати Google, але приховує дані користувача.

YaCy – децентралізована пошукова система з відкритим кодом.

Використання Tor Browser дозволяє здійснювати пошук анонімно та обходити цензуру.

Таким чином, сучасний пошук в Інтернеті розвивається у двох напрямках: з одного боку – більш точні та швидкі алгоритми (Google, Bing), а з іншого – зростає попит на захист конфіденційності (DuckDuckGo, Tor)

1. Базові поняття та методи соціальної інженерії: фішингові імейли, сайти та заражене програмне забезпечення

Соціальна інженерія – це наука, яка вивчає людську поведінку та фактори, які на неї впливають. Вона була створена для дослідження та вивчення людської поведінки. Наразі її активно використовується для планування та проведення кібератак. В цьому контексті соціальна інженерія - це техніки впливу та маніпулювання людьми, щоб здобути довіру або переконати їх виконати певні дії. Цей підхід ґрунтується не на технічних вразливостях, а на експлуатації людських слабкостей, як-от довірливість чи страх. Він побудований на розумінні психології людини та використанні цих знань для досягнення конкретних цілей: отримання даних для входу на сайт, вимагання грошей чи поширення особистих фотографій.

Існує декілька методів використання соціальної інженерії:

1. Без прямого контакту з цільовою особою. Цей метод полягає у використанні особистої інформації для підбирання паролів (день народження, імена членів родини або номер телефону). Також злочинці можуть маніпулювати системами відновлення паролів, відповідаючи на секретні питання, як-от про дівоче прізвище матері.

2. Без прямого контакту з цільовою особою, але через третіх сторін. Цей метод складається зі звернень до служб підтримки, друзів, знайомих або родичів людини, щоб отримати інформацію або вплинути на них так, щоб ті виконали певні дії, наприклад, надали конфіденційну інформацію.

3. Під час прямої комунікації з цільовою особою. Цей метод застосовується у тому випадку, коли шахрай вдає з себе представника служби підтримки, керівника, поліцейського або іншу особу, щоб переконати жертву надати конфіденційну інформацію або виконати дії, які можуть бути шкідливими для неї.

Методи соціальної інженерії: фішингові імейли, сайти та заражене програмне забезпечення»

Соціальна інженерія – це методи маніпуляцій людьми, щоб примусити їх розголосити конфіденційну інформацію або виконати певні дії. Замість того, щоб зламувати захист IT-систем, зловмисники намагаються «зламати» самих користувачів.

Типові методи соціальної інженерії містять фішинг, видавання себе за іншу людину, шантаж, пропонування хабарів тощо. Мета одна - маніпулювати жертвою аби отримати потрібні дані чи доступ.

Існує кілька видів застосування методів соціальної інженерії:

Фішингові імейли (рис. 1).

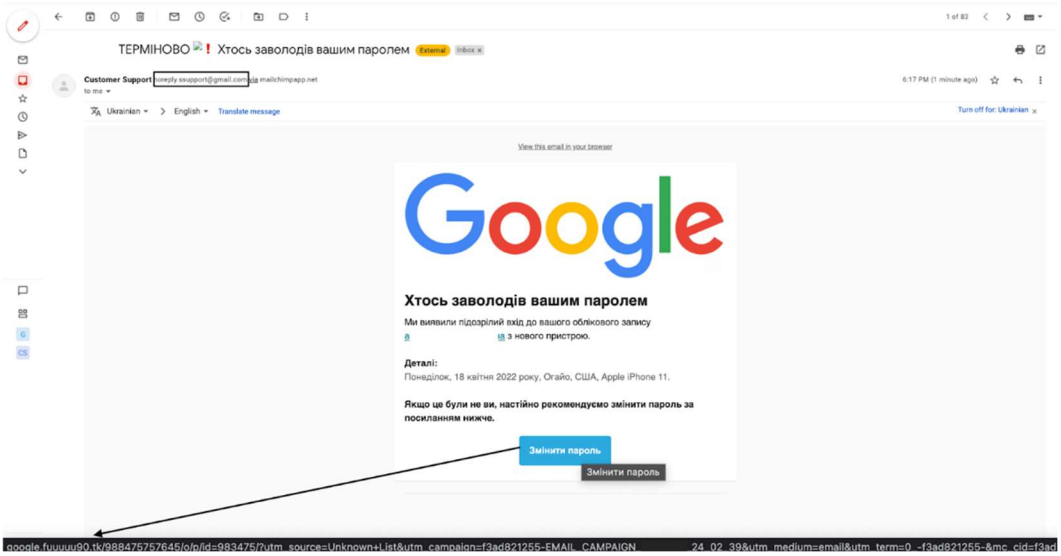

Рис. 1. Загальний вигляд фішингового імейлу.

Найчастіше вони потрапляють у спам, але трапляються винятки, тож слід бути вкрай обачними. Ось, наприклад, електронний лист, який спонукає змінити пароль та має всі ознаки фішингу, які ви дізналися раніше.

Фейкові сайти

Вони можуть виглядати як легітимні та з’являтися в результатах пошуку. Аби переконатися, що сайт безпечний, використовуйте інструмент перевірки від Google, перевіряйте, чи є у нього сертифікат SSL (замочок) для захисту особистих даних. Будьте обачними з сайтами з незвичним дизайном та помилками в тексті, оскільки це ознаки того, що ресурси фейкові.

Неліцензійне програмне забезпечення (рис. 2).

Рис. 2. Загальний вигляд неліцензійне програмне забезпечення

Це програми, які використовуються без офіційної ліцензії або правового дозволу. Восени 2022 року через торент-трекери поширювали неліцензійну заражену вірусом версію Windows 10, щоб збирати дані та атакувати працівників урядових установ України.

Фішинг у месенджерах. (рис. 3).

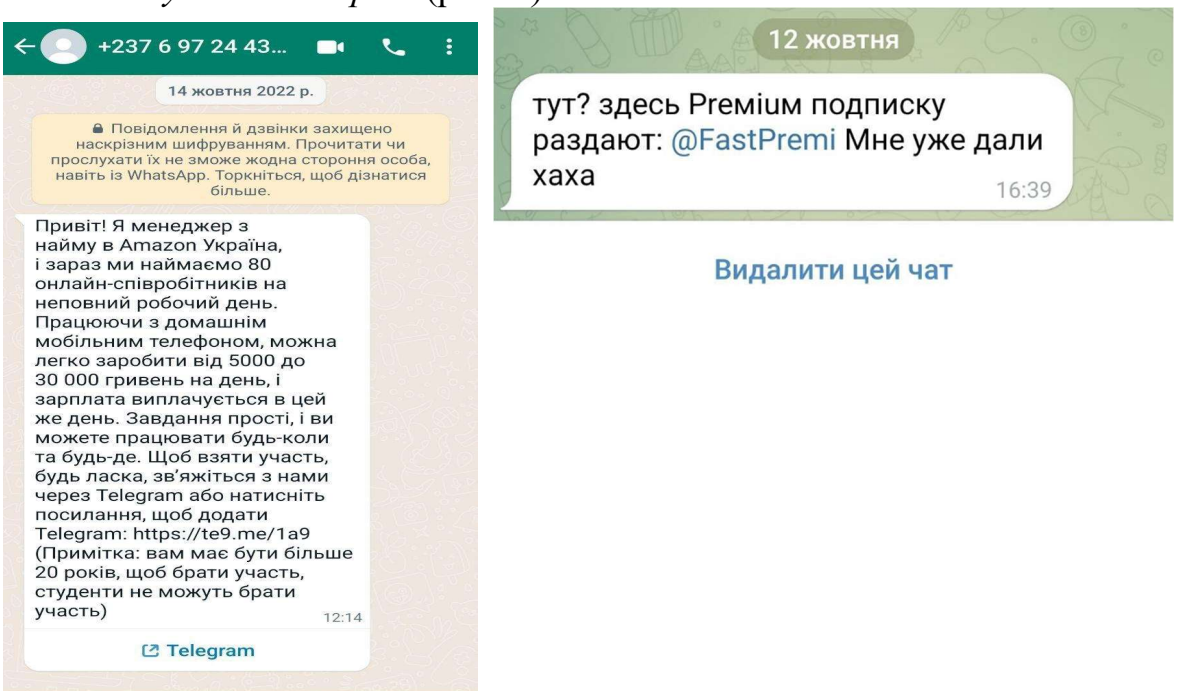

Рис. 3. Загальний вигляд фішингових листів у месенджерах.

Це вид атаки, при якому зловмисники надсилають оманливі повідомлення, що намагаються змусити користувачів до взаємодії, надаючи фальшиву інформацію чи покликання.

Наприклад, восени 2022 року шахраї використовували месенджери WhatsApp та Telegram для того, щоб заволодіти обліковими записами користувачів. Вони пропонували фальшиві пропозиції з вакансіями та безплатну підписку на Telegram Premium. Жертви мали перейти за покликанням чи авторизуватися. Так зловмисники отримували доступ до облікових записів.

Інструменти, що допоможуть розпізнати фейкові сайти:

Google Transparency Report – цей інструмент дозволяє перевірити, чи вважає Google сайт безпечним. Він надає звіти про безпечні вебперегляди та завантаження файлів.

Web Of Trust – цей сервіс – розширення для Google Chrome. Він оцінює вебсайти на основі відгуків користувачів та інформації про репутацію, щоб допомогти ідентифікувати ненадійні та потенційно шкідливі сайти.

VirusTotal – цей онлайн-інструмент дозволяє перевірити підозрілі файли та URL-адреси за допомогою декількох антивірусних двигунів та вебсайтів, що виявляють віруси, шкідливе програмне забезпечення та інші загрози.

ScamAdviser – цей інструмент допоможе проаналізувати інформацію стосовно домену та часу створення сайту. Ви самостійно приймаєте рішення, чи є аналізований сайт фейковим.

Who.is – цей інструмент надає детальну інформацію про власників домену, включно з датою реєстрації, контактними даними та іншими важливими деталями про доменні імена.

2. Безпека в інтернеті: онлайн-репутація, шкідливий онлайн-контент, секстинг, сексторшен, кіберсталкінг»

Кожна людина стикається з онлайн-простором, спілкуючись, купуючи товари та виконуючи інші дії через інтернет. Важливо пам'ятати про безпеку в цьому середовищі. Адже там необхідно дбати про свою онлайн-репутацію, остерігатися впливу шкідливого контенту, секстингу і сексторшену та кіберсталкінгу. Все, що ми робимо в інтернеті, позначається на нашій онлайн-репутації. А це і собі може сильно вплинути на наше життя, наприклад, на кар'єру та особисті стосунки.

Для перевірки та керування своєю онлайн-репутацією рекомендується:

– пошукати інформацію про себе в різних пошукових системах, використовуючи різні ідентифікаційні дані, як-от нікнейм або місце роботи;

– перевірити згадки про себе в Google Фото;

– проаналізувати свої соціальні мережі та видалити контент, який може негативно вплинути на вашу онлайн-репутацію.

В інтернеті можна знайти як корисну інформацію, так і шкідливу. До шкідливого онлайн-контенту відносять матеріали, які спонукають до

самопошкодження чи суїциду, а також ті, що пропагують насильство, порнографію та незадоволення зовнішністю, призводячи до розладів харчової поведінки.

Якщо ви відчуваєте вплив шкідливого онлайн-контенту, то поділіться проблемою з рідними або довіреними особами та складіть план виходу з цієї ситуації. За потреби, можна звернутися до правоохоронних органів і подати скарги на вебплатформу, де його розміщують. При потребі зверніться за психологічною підтримкою на спеціалізовані гарячі лінії або на сторінки цих організацій в соціальних мережах.

Важливо також знати про секстинг та сексторшен та як боротися з ними, якщо ви потерпіли від цих явищ.

Секстинг – це обмін інтимними фото чи відео, або ведення інтимного листування. Він може призвести до розповсюдження інтимного контенту без згоди особи та викликати сексуальне насильство, як віртуальне, так і реальне.

Сексторшен – це шантаж публікуванням сексуального контенту, щоб залякати людину чи примусити її до певних дій.

РЕКОМЕНДАЦІЇ

Якщо хтось поширює ваші інтимні фото чи відео без згоди:

1. Зробіть скриншоти сторінки з вашими фото чи відео.
2. Попросіть адміністрацію соціальної мережі або сайту видалити цей контент.
3. Зверніться із заявою до правоохоронних органів та проінформуйте, що ці фото чи відео опублікували без вашої згоди на це.
4. За секстинг і сексторшен зловмисника або зловмисницю можуть притягнути до відповідальності за статтями Кримінального кодексу України.
5. Окрім цього, за даними опитування 2017 року, 23 % жінок зазнавали кіберсталкінгу хоча б один раз за своє життя. Кіберсталкінг - це форма психологічного насильства, що характеризується переслідуванням або домаганням людини в інтернеті.
6. Для захисту зробіть скриншоти погроз та зверніться до поліції. Уникайте будь-якої комунікації з кіберсталкером чи кіберсталкеркою та поскаржтеся в соцмережах на повідомлення від такої людини. Поділіться проблемою з довіреною особою, зверніться за психологічною підтримкою, якщо маєте таку потребу.

Віртуальний світ вимагає уваги до особистої онлайн-репутації та захисту від шкідливого контенту. Перевіряйте та керуйте своєю репутацією, реагуйте на шкідливий контент та повідомлення, а за потреби звертайтеся до правоохоронних органів, аби припинити насильство у ваш бік.

3. Безпека в інтернеті: кібербулінг, кібергрумінг, тролінг, флеймінг, хепіслепінг, хейтспіч, доксинг, кетфішинг

З цього модуля ви дізналися про секстинг, сексторшен та кіберсталкінг. Але існує ще багато форм кібернасильства, з якими можна зіткнутися кожного дня. Ось перелік найпоширеніших.

Кібербулінг – цькування людини (найчастіше використовується в контексті дітей) через поширення образливих повідомлень або залякування через соціальні мережі. В Україні існує закон згідно з яким булер чи булерка або їхні батьки несуть адміністративну відповідальність у вигляді штрафу та виправних робіт.

Кібергрумінг – входження в довіру до дитини, з метою її схилення до якого-небудь брутального поводження з сексуальним підтекстом і подальшої реальної зустрічі з дитиною для сексуальних цілей.

Тролінг – розміщення в інтернеті провокаційних повідомлень. Наприклад, щоб викликати конфлікт чи взаємні образи між учасниками / учасницями розмови.

Флеймінг – обмін гнівними повідомленнями в інтернет-дискусіях.

Хепіслепінг – відеоролики, які найчастіше знімають підлітки, з записами реальних сцен насильства, в тому числі стосовно дорослих людей.

Хейтспіч (мова ворожнечі) – це агресивні висловлювання, які принижують та дискримінують людину чи групу людей за різними ознаками. Існує безліч видів мови ворожнечі, наприклад, за расою, статтю чи віком.

Доксинг – це збір і висвітлення у публічному просторі особистої інформації про людину, групу людей чи організацію без їхньої згоди.

Кетфішинг – створення фейкових профілів у соціальних мережах чи сайтах для онлайн-знайомств для обману та шахрайства, або просто видавання себе за іншу людину.

Завдання:

Завдання 1. Ознайомлення з пошуковими системами. Визначте, які пошукові системи використовувалися на початковому етапі розвитку Інтернету.

1. Знайдіть у Google інформацію про алгоритм PageRank.

Завдання 2. Використання Google для спеціалізованого пошуку

1. За допомогою Google Scholar знайдіть 2 наукові статті з теми «OSINT-технології».

2. Використайте оператор filetype:pdf для пошуку звітів з інформаційної безпеки.

3. Виконайте пошук за допомогою site:gov.ua для знаходження офіційних документів.

Завдання 3. Робота з іншими системами пошуку

1. Використайте DuckDuckGo для пошуку інформації про анонімність в Інтернеті.

2. Зробіть пошук тієї ж теми через Startpage та порівняйте результати.

Завдання 4. Перевірка достовірності інформації

1. Виберіть одну новину з результатів пошуку.
2. Визначте першоджерело публікації.
3. Зіставите знайдені відомості у 2–3 різних пошукових системах.

Приклад виконання завдань наведено у додатку 5.

Завдання 5. Пройти тест за темою

Вимоги до оформлення практичної роботи

Загальні вимоги

Робота виконується українською мовою.

Обсяг – 5–8 сторінок друкованого тексту (без урахування додатків).

Формат аркуша – А4.

Поля: верхнє та нижнє – 20 мм, ліве – 25 мм, праве – 15 мм.

Шрифт – Times New Roman, розмір – 14 pt.

Міжрядковий інтервал – 1,5.

Вирівнювання тексту – по ширині.

Абзацний відступ – 1,25 см.

Структура роботи

Титульна сторінка

Назва міністерства

Назва закладу освіти.

Назва дисципліни.

Назва практичної роботи (№, тема).

Прізвище, ім’я студента.

Група, курс.

ПІБ викладача.

Рік та місто.

Мета роботи – коротке формулювання (2–3 речення).

Завдання роботи – перелік завдань, які необхідно виконати.

Хід виконання роботи – опис дій здобувача: приклади пошукових запитів, результати, спостереження (можна додавати скріншоти).

Аналіз та обговорення результатів – оцінка отриманої інформації, перевірка достовірності, порівняння різних пошукових систем.

Висновки – узагальнення результатів (не менше ніж 0,5 сторінки).

Список використаних джерел – оформлюється згідно з ДСТУ 8302:2015 (оформлення бібліографічних посилань).

Додатки (за потреби) – скріншоти, таблиці, діаграми, схеми.

Оформлення ілюстрацій та таблиць

Ілюстрації (схеми, графіки, скріншоти) нумеруються:

Рис. 1.1 – Приклад пошукового запиту.

Таблиці також нумеруються та мають назву: *Таблиця 1 – Результати пошуку в Google*.

Посилання на рисунки та таблиці обов’язкові в тексті.

Вимоги до стилю викладу

Текст має бути науково-діловим, без жаргонізмів. Використовуються чіткі, логічні формулювання. При цитуванні обов'язкове посилання на джерело.

Контрольні питання

1. Які етапи розвитку пошукових систем можна виділити?
2. Чим відрізняється Google від перших пошукових систем?
3. Для чого застосовуються пошукові оператори (site:, filetype: тощо)?
4. Що таке мета-пошукові системи та в чому їх переваги?
5. Які системи анонімного пошуку ви знаєте?
6. Як перевірити достовірність знайденої інформації?
7. Що таке індексація веб-сторінок і як вона впливає на результати пошуку?
8. Які особливості ранжування результатів у сучасних пошукових системах?
9. Що таке «Google Dork» і як його можна застосовувати для пошуку інформації?
10. Які ризики та обмеження пов'язані з використанням відкритих джерел у пошуку інформації?

Список використаних джерел до теми 4

1. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с. URL : https://er.dduvs.edu.ua/handle/123456789/7110 (дата звернення 24.04.2026).
2. Інформаційні та комунікаційні технології : навч. посіб. / О. А. Дісковський, Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов. Дніпро: Дніпров. держ. ун-т внутр. справ, 2025. 272 с. URL : https://er.dduvs.edu.ua/handle/123456789/16603 (дата звернення 24.04.2026).
3. ISO/IEC 27043:2015. Information technology. Security techniques. Incident investigation principles and processes [Електронний ресурс]. ISO/IEC. URL : https://webstore.iec.ch/en/publication/24354 (дата звернення 24.04.2026).
4. UNESCO; International Association of Prosecutors. Guidelines for prosecutors on digital evidence collection in compliance with international standards on freedom of expression and privacy [Електронний ресурс]. UNESCO. URL : https://unesdoc.unesco.org/ark%3A/48223/pf0000395060 (дата звернення 24.04.2026).
5. Синиціна Ю. П. Автоматизовані інформаційні системи в правоохоронній діяльності Економічна та інформаційна безпека: актуальні питання та інновації: Всеукр. наук.-практ. конф. (м. Дніпро, 04 листопада 2021 р.,). Дніпро: ДДУВС, 2021. С. 220-222 URL : https://ibn.idsi.md/sites/default/files/imag_file/_%D0%BA%D0%BE%D0%BD%

D1%84_%D0%95%D0%86%D0%91-04.11.2021.pdf#page=220 (дата звернення: 24.04.2026).

6. Інформаційно-пошукова правова система «Нормативні акти України» (НАУ). URL : http://www.nau.ua/.

7. Офіційний сайт Єдиного державного веб-порталу відкритих даних: URL : https://data.gov.ua/.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ КІБЕРГІГІЄНИ»

1. Що таке кібергігієна і чому вона важлива для сучасного користувача? Назвіть основні складові кібергігієни.
2. Які основні кіберзагрози існують у сучасному цифровому середовищі?
3. Наведіть приклади фізичних і цифрових загроз для персональних пристроїв.
4. Які принципи безпечного використання персональних пристроїв слід дотримуватися?
5. Поясніть поняття «інформаційна безпека» та її основні цілі.
6. Які наслідки можуть бути у разі порушення кібергігієни?
7. Що таке надійний пароль і які правила його створення?
8. Навіщо потрібна двофакторна аутентифікація (2FA)? Назвіть види двофакторної аутентифікації.
9. Які основні загрози існують у соціальних мережах щодо персональних даних?
10. Що таке політика приватності у хмарних сервісах?
11. Наведіть приклади методів шифрування даних.
12. Як безпечно зберігати інформацію на персональному пристрої та у хмарі?
13. Які ризики виникають при використанні однакових паролів на різних сервісах?
14. Яким чином можна перевірити надійність свого пароля?
15. Назвіть основні види шкідливого програмного забезпечення.
16. В чому відмінність вірусу, трояна і шпигунської програми?
17. Що таке фішинг і як його розпізнати?
18. Поясніть поняття «соціальна інженерія» та наведіть приклади.
19. Які основні принципи антивірусного захисту?
20. Чому важливо регулярно оновлювати програмне забезпечення?
21. Назвіть приклади безпечної поведінки у мережі для запобігання кібератакам.
22. Як можна перевірити, що файл чи посилання безпечні перед відкриттям?
23. Як розвивалася історія пошукових систем та які основні етапи їх розвитку?
24. Назвіть основні сервіси Google, що використовуються для пошуку інформації.
25. Що таке мета-пошукові системи і чим вони відрізняються від звичайних?

26. Як забезпечити анонімний пошук інформації в Інтернеті?

27. Як шукати оперативну інформацію у Facebook та інших соціальних мережах?

28. Які основні правила особистої безпеки під час користування Інтернетом та чат-ботами в месенджерах, таких як Telegram?

ПЕРЕЛІК ОСНОВНОЇ ЛІТЕРАТУРИ ДО ДИСЦИПЛІНИ «ОСНОВИ КІБЕРГІГІЄНИ»

Основні нормативні акти:

закони:

1. Про адвокатуру та адвокатську діяльність: Закон України від 05.07.2012 № 5076-VI. Редакція від 15.11.2024. URL : https://zakon.rada.gov.ua/laws/show/5076-17#Text (дата звернення 24.04.2026);

2. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 24.04.2026).

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 24.04.2026).

4. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. Редакція від 31.12.2023. URL : https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 24.04.2026).

5. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI редакція від 01.08.2025. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 24.04.2026).

6. Цивільний процесуальний кодекс України від 18.03.2004 № 1618-IV редакція від 17.07.2025. URL : https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення 24.04.2026).

7. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR) [Електронний ресурс]. URL : https://gdprinfo.eu/ (дата звернення 24.04.2026).

8. Європейська конвенція про захист прав людини і основоположних свобод Рада Європи. Європейська конвенція про захист прав людини і основоположних свобод (European Convention on Human Rights) [Електронний ресурс]. URL : https://www.echr.coe.int/d/convention_ukr (дата звернення 24.04.2026).

9. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI [Електронний ресурс] / European Commission. URL : https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата звернення 24.04.2026).

10. Регламент (ЄС) 2024/1689 Європейського парламенту і Ради від 13 червня 2024 р. про гармонізовані правила щодо штучного інтелекту (Artificial Intelligence Act) [Електронний ресурс]. URL : https://aiactinfo.eu/ (дата звернення 24.04.2026).

11. Організація Об'єднаних Націй. Цілі сталого розвитку (Sustainable Development Goals) [Електронний ресурс]. URL: https://sdgs.un.org/ru/goals (дата звернення 24.04.2026).

12. ЮНЕСКО. Recommendation on the Ethics of Artificial Intelligence [Електронний ресурс]. URL: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence (дата звернення 24.04.2026);

13. Government of Canada. Canada's Artificial Intelligence Strategy for the Federal Public Service [Електронний ресурс] / Government of Canada. URL : https://www.canada.ca/en/treasury-board-secretariat/news/2025/03/canada-launches-first-ever-artificial-intelligence-strategy-for-the-federal-public-service.html (дата звернення 24.04.2026);

14. White House Office of Science and Technology Policy. Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People [Електронний ресурс]. URL : https://data.aclum.org/storage/2025/01/OSTP_www_whitehouse_gov_ostp_ai-bill-of-rights.pdf (дата звернення 24.04.2026).

15. ISO/IEC 27037:2012. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence [Електронний ресурс]. ISO. URL : https://www.iso.org/ru/standard/44381.html (дата звернення 24.04.2026).

16. ISO/IEC 27042:2015. Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence [Електронний ресурс]. ISO. URL: https://www.iso27001security.com/html/27042.html (дата звернення 24.04.2026).

17. ISO/IEC 27043:2015. Information technology. Security techniques. Incident investigation principles and processes [Електронний ресурс]. ISO/IEC. URL : https://webstore.iec.ch/en/publication/24354 (дата звернення 24.04.2026).

18. United Nations General Assembly Resolution 78/213. Promotion and protection of human rights in the context of digital technologies [Електронний ресурс]. United Nations. URL: https://docs.un.org/A/RES/78/213 (дата звернення 24.04.2026).

19. UNESCO; International Association of Prosecutors. Guidelines for prosecutors on digital evidence collection in compliance with international standards on freedom of expression and privacy [Електронний ресурс]. UNESCO. URL: https://unesdoc.unesco.org/ark%3A/48223/pf0000395060 (дата звернення 24.04.2026).

постанови, інші рішення, роз'яснення суддів (Конституційного, Верховного):

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних система: Постанова КМУ від 8 лютого 2021 року № 92. URL : https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text (дата звернення 24.04.2026).

2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС

України від 03.08.2017 № 676. Дата оновлення: 01.04.2022. URL : https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення 24.04.2026).

3. Кабінет Міністрів України. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження від 02.12.2020 № 1556-р [Електронний ресурс]. База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/go/1556-2020-%D1%80 (дата звернення 24.04.2026).

Підручники:

1. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с. URL : https://er.dduvs.edu.ua/handle/123456789/7110 (дата звернення 24.04.2026).

2. Інформаційні технології: підруч. / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро: Дніпр. держ. ун-т внутр.справ, 2021. 492 с. URL : https://er.dduvs.edu.ua/handle/123456789/6820 (дата звернення 24.04.2026).

Навчальні посібники, інші дидактичні та методичні матеріали:

1. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 181 с. URL : https://er.dduvs.edu.ua/handle/123456789/15045 (дата звернення 24.04.2026).

2. Інформаційні та комунікаційні технології : навч. посіб. / О. А. Дісковський, Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов. Дніпро: Дніпров. держ. ун-т внутр. справ, 2025. 272 с. URL : https://er.dduvs.edu.ua/handle/123456789/16603 (дата звернення 24.04.2026).

3. Бутенко Т. А. Сирий В. М. Інформаційні системи та технології : навчальний посібник - Харків: ХНАУ ім. В. В. Докучаєва, 2020. 207 с.

Монографії та інші наукові видання:

1. Впровадження сучасних систем цифрового радіозв’язку у підрозділах Національної поліції: наук.-практ. рекоменд. / В. О. Мирошниченко, С. О. Прокопов, Е. В. Рижков, Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 29 с.;

2. Синиціна Ю. П., Станіна О. Д. Обґрунтування актуальності цифрової комунікація закладів вищої освіти (Rationale for the relevance of digital communication in higher education institutions) Міжн. колект.моногр. / Selected aspects of digital society development «Digital Economyand Digital Society» III Міжнародна конференція (28-29 травня 2021 р.) Katowice, University of Technology, Poland, 2021.mon # 45. 148-156 с., URL:

http://www.wydawnictwo.wst.pl/uploads/files/337190b4d66761009188e7904791336d.pdf (дата звернення: 24.04.2026).

3. Штучний інтелект: що змінилося за 50 років / Ю. П. Синиціна, Е. В. Рижков, О. Д. Станіна. Theoretical foundations of engineering. Tasks and problems : collective monograph / Boiko T., Boiko P., etc. Boston : Primedia eLaunch, 2021. 485 p. DOI: https://doi.org/10.46299/ISG.2021.MONO.44TECH.III.

4. Синиціна Ю. П., Бекишев А. Методологічні аспекти цифрової комунікації закладів вищої освіти. Науковий вісник, м. Дніпро, 2021, № 3, С. 340-348; ISSN – 2078-3566; «Index Copernicus International» «CrossRef». DOI: https://doi.org/10.31733/2078-3566-2021-3-340-348.

Інші джерела:

1. Ковальова О. В. Інформаційне забезпечення професійної діяльності: навч. посіб. Київ: «Дакор», 2021. 288 с.

2. Сучасна концепція реформування судоустрою, судочинства та суміжних правових інститутів [Електронне видання] : навчально-методичний посібник (для здобувачів ступеня доктора філософії денної, вечірньої та заочної форми навчання) / Н.М. Бакаянова, А. В. Кубаєнко, І.О. Кісліцина. Одеса: Фенікс, 2021. 157 с. URL : http://dspace.onua.edu.ua/ (дата звернення 24.04.2026).

3. Синиціна Ю. П., Причина В. Р. Оцінка системи управління інформаційної безпеки методом таксономії Nauka i edukacja w warunkach zmian cywilizacyjnych: Mater. II Międz. Konf. Nauk.-Prakt. / Pod red. Stanisława Kowalczyka – Łódź: Nowa nauka, 2020, p. 76 – 78 ISBN 978-83-7364-968-2.

4. Синиціна Ю. П. APT-атак – пріоритетний напрямок розвитку кібербезпеки Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф. 19.12. 2020 р., м. Львів : ЛьвДУВС, 2020. с. 66-68 URL: https://www2.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/19_12_2020.pdf (дата звернення: 24.04.2026).

5. Синиціна Ю. П. Сучасні підходи до безпеки операційних систем Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро: ДДУВС, 2020. с. 66-68; URL : https://er.dduvs.edu.ua/bitstream/123456789/5964/1/8.pdf (дата звернення: 24.04.2026).

6. Синиціна Ю. П., Дудник В. В. Актуальні питання взаємозв'язку інформаційної та національної безпеки України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро: ДДУВС, 2020. с. 164-167 URL : https://er.dduvs.edu.ua/bitstream/123456789/5920/1/44.pdf (дата звернення: 24.04.2026).

7. Синиціна Ю. П., Кліменко А. О. Актуальні питання інформаційної безпеки в діяльності Національної поліції України Сучасні інформаційні

технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро: ДДУВС, 2020. с. 174-176. URL : https://er.dduvs.edu.ua/bitstream/123456789/5918/1/46.pdf (дата звернення: 24.04.2026).

8. Синиціна Ю. П. Автоматизовані інформаційні системи в правоохоронній діяльності Економічна та інформаційна безпека: актуальні питання та інновації: Всеукр. наук.-практ. конф. (м. Дніпро, 04 листопада 2021 р.,). Дніпро: ДДУВС, 2021. С. 220-222 URL: https://ibn.idsi.md/sites/default/files/imag_file/_%D0%BA%D0%BE%D0%BD%D1%84_%D0%95%D0%86%D0%91-04.11.2021.pdf#page=220 (дата звернення: 24.04.2026).

9. Синиціна Ю. П. Державного управління забезпечення національної безпеки: інформаційна безпека Міжнародна та національна безпека: теоретичні і прикладні аспекти: VI Міжн. наук.-практ. конф. м. Дніпро, 11 березня 2022р.,). Дніпро: ДДУВС, 2022. С. 263-266 URL : https://er.dduvs.edu.ua/handle/123456789/9735 (дата звернення: 24.04.2026).

10. Синиціна Ю. П. Інформаційна безпека в умовах воєнного стану / Ю. П. Синиціна // Сучасні пріоритети розвитку України: економічна та інформаційна безпека : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 10 жовтня 2023 р.). Дніпро : ДДУВС, 2024. С. 40-42. URL: https://er.dduvs.edu.ua/handle/123456789/15030 (дата звернення: 24.04.2026).

11. Синиціна Ю. П. Інформаційна безпека у системі права національної безпеки України Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об’єктів права інтелектуальної власності: зб. наук.праць за матеріал. IV Міжн. наук.-практ. інтер.-конф. (24-25 березня 2022р.). УДУНТ, УКРНЕТ, НДІІВ НАПрН України, Дніпро: Юрсервіс, 2022. С. 165 – 168.

Інтернет-ресурси:

1. Інформаційно-пошукова правова система «Нормативні акти України» (НАУ). URL : http://www.nau.ua.

2. Офіційний сайт Національної поліції України. URL : https://www.npu.gov.ua/.

3. Офіційний сайт Єдиного державного веб-порталу відкритих даних. URL : https://data.gov.ua/.

4. Офіційний сайт Міністерства внутрішніх справ України. URL : https://www.mvs.gov.ua/.

5. Бібліотека ХНУВС. URL : https://lib.univd.edu.ua/.

СИСТЕМА ОЦІНЮВАННЯ УСПІШНОСТІ З ДИСЦИПЛІНИ «ОСНОВИ КІБЕРГІГІЄНИ»

Для навчальної дисципліни «Основи кібергігієни» засобами діагностики знань (успішності навчання) виступають: лекційні, семінарські та практичні заняття, самостійна робота і підсумковий контроль.

ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		**Підсумковий контроль**
Аудиторна робота	Самостійна робота/ Індивідуальна робота	ЕКЗАМЕН (Е)
≤ 20	≤ 30	
≤ 50		≤ 50
Підсумкова оцінка у випадку складання екзамену (П) ПК + Е ≤ 100		

Критерієм успішного проходження здобувачем підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Мінімальний пороговий рівень оцінки визначається за допомогою якісних критеріїв і трансформується в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали.

Здобувач допускається до складання підсумкового контролю, якщо ним виконані всі передбачені РПНД поточні завдання та сума балів поточного контролю не менше ніж 34. Якщо сума балів поточного контролю менше ніж 34, здобувач не допускається до підсумкового контролю і зобов'язаний доопрацювати завдання та набрати необхідну кількість балів.

За результатами аудиторної роботи здобувач заочної форми навчання має отримати максимальну кількість 20 балів (кожне заняття оцінюється за п'ятибальною шкалою); за результатами самостійної роботи – 30 балів. Таким чином бали за поточний контроль (34-50 балів).

Розрахунок підсумкової оцінки з навчальної дисципліни «Основи кібергігієни» здійснюється відповідно до формули:

П ПК+Е≤100,

де ПК – бали за поточний контроль (34-50 балів),
Е – бали за результатами складання екзамену

Критерії оцінювання аудиторної роботи здобувачів вищої освіти (заочна форми навчання)

БАЛИ	ПОЯСНЕННЯ
5	**Високий рівень** компетентностей. Питання, винесені на розгляд, **засвоєні у повному обсязі; на високому рівні сформовані**

БАЛИ	ПОЯСНЕННЯ
	необхідні практичні навички та вміння; **всі** навчальні завдання, передбачені планом заняття, **виконані** в повному обсязі. Під час заняття продемонстрована стабільна активність та ініціативність. Відповіді на теоретичні питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань ґрунтується **на глибокому знанні** чинного законодавства, теорії та правозастосовної практики.
4	**Невисокий рівень** компетентностей. Питання, винесені на розгляд, **засвоєні у повному обсязі; в основному сформовані** необхідні практичні навички та вміння; **всі** передбачені планом заняття навчальні завдання **виконані** в повному обсязі **з неістотними неточностями**. Під час заняття продемонстрована ініціативність. Відповіді на питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань **переважно ґрунтується на знанні** чинного законодавства, теорії та правозастосовної практики.
3	**Достатній рівень** компетентностей. Питання, винесені на розгляд, **загалом засвоєні**; практичні навички та вміння мають **поверхневий характер**, потребують подальшого напрацювання та закріплення; навчальні завдання, передбачені планом заняття, **виконані**, **деякі** види завдань виконані **з помилками**.
2	**Недостатній рівень** компетентностей. Питання, винесені на розгляд, **засвоєні частково**, **прогалини** у знаннях **не носять істотного характеру**; практичні навички та вміння **сформовані недостатньо**; **більшість** навчальних завдань **виконано, деякі** з виконаних завдань **містять істотні помилки,** які потребують подальшого усунення.
1	**Мінімальний рівень** компетентностей. Студент, не готовий до заняття, не знає більшої частини програмного матеріалу, з труднощами виконує завдання, невпевнено відтворює терміни і поняття, що розглядалися під час заняття, допускає змістовні помилки, не володіє відповідними вміннями і навичками, необхідними для розв'язання професійних завдань.
0	**Незадовільний рівень** компетентностей. Відсутність на занятті.

Для навчальної дисципліни «Основи кібергігієни» засобами діагностики знань (успішності навчання) виступають: стандартизовані тести, тези, есе, презентації результатів виконаних завдань та досліджень, презентації та виступи на наукових заходах, інші види індивідуальних та групових завдань.

Критерії оцінювання самостійної роботи (заочна форма навчання)

Пропонується наступне оцінювання самостійної роботи здобувачів вищої освіти за виконання 1 завдання за вибором здобувача вищої освіти та узгодженням з викладачем для отримання максимальної кількості балів - 30:

1. Написання та участь у конкурсі творчих та/або наукових робіт серед здобувачів вищої освіти (МОН, ДДУВС) (написання робіт, есе, доповідь, творча публікація, творча візуалізація, відеоролик) - 30 балів.

2. Підготовка презентацій-доповідей участі в роботі науковому студентську гуртку кафедри (надати презентація та фото виступу) – 30 балів.

3. Підготовка тези доповідей на міжнародну (всеукраїнську) науково-практичну конференцію за умови надання PrinScrin перевірки на плагіат за результатом не менше 70 % оригінального тексту. Тези повинні бути підготовленні відповідно «Методичних вказівок з написання тез» – 30 балів.

4. Отримання сертифікату після проходження он-лайн тесту Цифрограм 1.0 для громадян на освітній платформі ДІЯ: Освіта https://osvita.diia.gov.ua/digigram – 30 балів.

5. Підготовка презентації у редакторі Google презентації (завантаження презентації та надання посилання у коментарях) за темою зі списку у додатковому файлі «Методичні вказівки до виконання презентації у редакторі Google презентація» – 30 балів.

6. Проходження тесту з самостійної роботи - 30 балів.

Шкала оцінювання: національна та ECTS

Оцінка в балах	**Оцінка за національною шкалою**		**Оцінка за шкалою ECTS**	
	Залік	**Екзамен/ диференційований залік**	**Оцінка**	**Пояснення**
90-100	зараховано	Відмінно	A	«**Відмінно**» – теоретичний зміст курсу засвоєний у повному обсязі; сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані в повному обсязі.
83-89		Добре	B	«**Дуже добре**» – теоретичний зміст курсу засвоєний в повному обсязі; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання більшості з них оцінена кількістю балів, близько до максимальної.
75-82			C	«**Добре**» – теоретичний зміст курсу засвоєний цілком; в основному сформовані практичні навички роботи із засвоєним матеріалом; всі

				навчальні завдання, передбачені РПНД, виконані, якість виконання жодного з них не оцінена мінімальною кількістю балів, деякі види завдань виконані з помилками.
68-74		Задовільно	D	«**Задовільно**» – теоретичний зміст курсу засвоєний не повністю; але прогалини не носять істотного характеру; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; більшість передбачених РПНД навчальних завдань виконано, деякі з виконаних завдань містять помилки.
60-67			E	«**Достатньо**» – теоретичний зміст курсу засвоєний частково; не сформовано деякі практичні навички роботи; частина передбачених РПНД навчальних завдань не виконані або якість виконання деяких з них оцінено числом балів, близьким до мінімального.
35-59	не зараховано	Не задовільно	FX	«**Умовно незадовільно**» – теоретичний зміст курсу засвоєний частково; не сформовані необхідні практичні навички роботи; більшість навчальних завдань не виконано або якість їх виконання оцінено кількістю балів, близько до мінімальної; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання).
1-34			F	«**Безумовно незадовільно**» – теоретичний зміст курсу не засвоєний; не сформовані необхідні практичні навички роботи; всі виконані навчальні завдання містять грубі помилки або не виконані взагалі; додаткова самостійна робота над матеріалом курсу не призведе до значного підвищення якості виконання навчальних завдань.

СЛОВНИК ТЕРМІНІВ

ТЕМА 1. ВСТУП ДО КІБЕРГІГІЄНИ ТА ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кібергігієна – сукупність правил і практик безпечної поведінки користувача у цифровому середовищі, спрямованих на захист даних і пристроїв.

Кіберзагроза – потенційна дія або подія, яка може порушити конфіденційність, цілісність чи доступність інформації.

Шкідливе програмне забезпечення (Malware) – програми, створені для пошкодження пристроїв, крадіжки даних або несанкціонованого доступу (віруси, трояни, шпигунські програми).

Соціальна інженерія – метод обману користувачів для отримання конфіденційної інформації шляхом психологічного впливу (фішинг, шахрайські листи).

Фішинг – вид інтернет-шахрайства, коли зловмисники створюють підроблені сайти чи повідомлення для викрадення персональних даних.

Несанкціонований доступ – отримання доступу до інформаційних ресурсів чи акаунтів без дозволу власника.

DDoS-атака (Distributed Denial of Service) – масова атака на сервер чи мережу з метою виведення їх з ладу шляхом перевантаження.

Аутентифікація – процес перевірки особи користувача при доступі до системи (наприклад, за паролем чи 2FA).

Двофакторна аутентифікація (2FA) – метод захисту, що вимагає підтвердження входу за допомогою двох різних факторів (пароль + код із SMS або додатку).

VPN (Virtual Private Network) – технологія захищеного з’єднання, що забезпечує конфіденційність передавання даних через Інтернет.

ТЕМА 2. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЦИФРОВИХ ОБЛІКОВИХ ЗАПИСІВ

Пароль – секретна комбінація символів, яка використовується для автентифікації користувача та захисту облікового запису.

Надійний пароль – пароль, що містить великі та малі літери, цифри та спеціальні символи, довжиною не менше 12 символів, і складно піддається злому.

Двофакторна аутентифікація (2FA) – додатковий рівень захисту облікового запису, який вимагає введення пароля та одноразового коду, отриманого через SMS або додаток-аутентифікатор.

Шифрування – процес перетворення даних у недоступний для сторонніх формат з метою забезпечення конфіденційності.

Дешифрування – процес відновлення зашифрованих даних у початковий вигляд за допомогою ключа.

Політика приватності – набір правил та налаштувань сервісу, що визначають порядок збору, обробки та захисту персональних даних користувача.

Обліковий запис (акаунт) – персональна цифрова ідентифікація користувача в сервісі, що дозволяє зберігати дані та отримувати доступ до ресурсів.

Менеджер паролів – спеціальний програмний інструмент для створення, зберігання та автоматичного введення надійних паролів.

Резервне копіювання (backup) – створення копій даних для їх відновлення у разі втрати, пошкодження або несанкціонованого доступу.

Фішинг – шахрайська техніка отримання конфіденційної інформації користувача через обман, наприклад, підроблені сайти або листи електронної пошти.

ТЕМА 3. КІБЕРЗАГРОЗИ ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ

Вірус – шкідлива програма, яка самостійно поширюється, вбудовуючись у файли чи системні області комп’ютера, з метою пошкодження даних або порушення роботи системи.

Троян (Trojan horse) – шкідливе програмне забезпечення, яке маскується під корисну програму, але виконує приховані дії: крадіжку паролів, встановлення бекдорів тощо.

Spyware (шпигунське ПЗ) – програма, яка таємно збирає інформацію про користувача (паролі, історію переглядів, натискання клавіш) і передає її зловмисникам.

Ransomware (програма-вимагач) – шкідливе ПЗ, яке блокує доступ до файлів або системи та вимагає викуп за їх відновлення.

Фішинг – вид шахрайства, при якому зловмисники видають себе за легітимні сервіси (банки, соцмережі) і виманюють у користувачів особисті дані.

Соціальна інженерія – методика впливу на людину з метою отримання конфіденційної інформації (наприклад, через телефонні дзвінки, підроблені листи, психологічний тиск).

DDoS-атака – атака на сервер або мережевий ресурс, що перевантажує його численними запитами та робить недоступним для користувачів.

Брандмауер (фаєрвол) – програмний чи апаратний засіб, що контролює та фільтрує вхідний і вихідний мережевий трафік для захисту системи.

Антивірус – програмне забезпечення, яке виявляє, блокує та видаляє шкідливі програми, забезпечуючи базовий рівень захисту комп’ютера.

Оновлення програмного забезпечення (патчі) – виправлення та доповнення, що випускаються розробниками для усунення вразливостей, підвищення безпеки та стабільності роботи програм.

ТЕМА 4. ПОШУК ПРАВОВОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ. ОСОБИСТА БЕЗПЕКА В ІНТЕРНЕТІ

OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел, тобто пошук, збір і аналіз інформації, яка є у вільному доступі.

Пошукова система – спеціалізований програмний комплекс для пошуку інформації в мережі Інтернет (наприклад, Google, Bing, Yahoo).

Спеціалізований пошук (Advanced Search) – використання логічних операторів та фільтрів для точнішого пошуку даних.

Метапошукова система – сервіс, що одночасно використовує кілька пошукових систем і видає зведені результати (наприклад, StartPage, DuckDuckGo).

Цифровий слід (Digital footprint) – інформація, яку користувач залишає про себе в Інтернеті (пости, фото, коментарі, історія пошуку тощо).

Анонімізація – методи приховування особистих даних і діяльності користувача в мережі (VPN, TOR, проксі-сервери).

Фішинг (Phishing) – вид кіберзлочину, що полягає у викраденні особистих даних шляхом маскування під надійні сервіси чи організації.

Соціальна інженерія – психологічні методи маніпуляцій для отримання конфіденційної інформації від користувачів.

Кібергігієна – комплекс правил безпечної поведінки в Інтернеті: використання надійних паролів, двофакторної автентифікації, перевірка посилань тощо.

Достовірність джерела – показник надійності та точності отриманої з відкритих ресурсів інформації, який перевіряється шляхом порівняння кількох незалежних джерел.

Додаток 1

ПРИКЛАД ФРАГМЕНТУ ПЕРСОНАЛЬНОГО ПЛАНУ КІБЕРГІГІЄНИ:

Періодичність	**Дії користувача**	**Інструменти/Примітки**
Щодня	Використання складних паролів, не відкривати підозрілі листи	Менеджер паролів, антивірус
Щотижня	Перевірка ПК на віруси, очищення кешу браузера	Антивірус, CCleaner
Щомісяця	Зміна паролів для критичних сервісів	Генератор паролів
Щорічно	Повний аудит акаунтів, перевірка резервних копій	Хмарні сервіси, зовнішній диск

Додаток 2

ПРИКЛАД УВІМКНЕННЯ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЯ (2FA)

Сервіс: Google
Метод: Google Authenticator
Кроки:
Налаштування → Безпека → Двофакторна аутентифікація
Сканування QR-коду додатком

Приклад увімкнення 2FA у Facebook
Сервіс: Facebook
Кроки виконання:
Увійдіть до свого облікового запису Facebook.
Перейдіть у Налаштування та конфіденційність → Налаштування → Безпека та вхід.
Знайдіть розділ Використання двоетапної аутентифікації та натисніть Редагувати.
Виберіть спосіб додаткової перевірки:
Додаток аутентифікації (Google Authenticator, Authy тощо)
SMS-коди на мобільний телефон
Якщо обрано додаток аутентифікації:
Відскануйте QR-код за допомогою додатку на смартфоні.
Введіть код, який згенерує додаток, для підтвердження активації.
Якщо обрано SMS-коди:
Введіть номер телефону для отримання кодів.
Введіть код, який прийшов у SMS, для підтвердження.
Після успішного налаштування двоетапна аутентифікація буде активована.
При наступному вході з нового пристрою Facebook запросить пароль + одноразовий код (2FA).
Результат:
Навіть якщо зловмисник дізнається ваш пароль, він не зможе увійти без одноразового коду з додатку або SMS.
Підвищено рівень безпеки облікового запису.

Додаток 3

ПРИКЛАД ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ ТЕМА № 3

1. Аналіз підозрілого листа (фішинг)

📧 Отриманий лист виглядав так:

Відправник: support@faceb00k-help.com (схожа, але підроблена адреса).

Тема: «Ваш акаунт буде видалено через порушення правил».

Текст: «Для підтвердження акаунта натисніть на посилання».

Посилання веде на сайт http://secure-facebook-login.net замість офіційного facebook.com.

Висновок: лист є прикладом фішингу, оскільки використовує підроблену адресу, помилки у тексті та підозріле посилання.

2. Перевірка файлів на віруси

Для перевірки використано сервіс VirusTotal.

Завантажений файл invoice_update.pdf.

Результат: 5 із 72 антивірусів виявили загрозу Trojan.PDF.Phishing.

Висновок: файл небезпечний, його відкривати не можна.

3. Налаштування антивірусного захисту

Антивірус: Windows Defender.

Перевірено налаштування:

Захист у реальному часі – увімкнено.

Автоматичні оновлення – активні.

Хмарний захист – активний.

Додатково увімкнено щотижневу повну перевірку системи.

4. Оновлення програмного забезпечення

Операційна система: Windows 10.

Перед початком – доступні 2 оновлення безпеки.

Після встановлення – система повідомила: «Ваше програмне забезпечення оновлене».

Висновок: регулярне встановлення оновлень знижує ризики зараження через вразливості.

Загальні висновки: Фішингові листи легко виявити за неприродними адресами та посиланнями. Перевірка файлів антивірусними сервісами допомагає уникнути зараження. Постійно активний антивірус та захист у

реальному часі – обов’язкові для будь-якого користувача. Оновлення операційної системи та програмного забезпечення є одним із найефективніших способів захисту від кіберзагроз.

Додаток 4

ПРИКЛАД ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ ТЕМА № 4

ТЕМА: ПОШУК ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ МЕРЕЖІ ІНТЕРНЕТ. ОСОБИСТА БЕЗПЕКА У ІНТЕРНЕТІ.

Мета роботи: **по**знайомитися з історією розвитку пошукових систем, навчитися користуватися базовими та спеціалізованими інструментами Google, а також перевіряти достовірність знайденої інформації.

Хід виконання роботи

Завдання 1. Ознайомлення з пошуковими системами

1. Перші пошукові системи: *Archie (1990), Lycos (1994), AltaVista (1995), Yahoo (1995).*

2. У Google знайдено інформацію про *PageRank* – алгоритм, що оцінює значущість веб-сторінки на основі кількості та якості посилань.

Завдання 2. Використання Google для спеціалізованого пошуку

1. *Google Scholar***:**

Запит: «OSINT technologies».

Знайдено статті:

«Open Source Intelligence (OSINT) in Cybersecurity» (2021).

«The Role of OSINT in Modern Security Analysis» (2020).

2. Пошук у Google за допомогою оператора filetype:

Запит: OSINT filetype:pdf.

Результат: «OSINT Tools and Techniques Report.pdf» (аналітичний звіт).

3. Пошук за допомогою site:

Запит: OSINT site:gov.ua.

Результат: публікації Міністерства цифрової трансформації України, новини CERT-UA.

Завдання 3. Робота з іншими системами пошуку

1. У *DuckDuckGo* за запитом “Internet anonymity” знайдено статті про VPN, Tor, анонімний пошук.

2. У *Startpage* за тим самим запитом результати були подібними, але з додатковим акцентом на інструменти шифрування та захисту даних.

Завдання 4. Перевірка достовірності інформації

1. Вибрано новину з Facebook: *«У місті Х зупинили метро через технічні несправності»*.

2. Перевірка:

Google News – підтверджено, що метро дійсно не працювало у зазначений час.

Telegram-канали – з’явилася інформація з офіційного джерела міської ради.

Висновок: інформація достовірна, але перше повідомлення було подане у перебільшеній формі.

ВИСНОВКИ: Історія пошукових систем показує еволюцію від простих каталогів до інтелектуальних алгоритмів Google. Оператори пошуку значно спрощують знаходження потрібних матеріалів. Мета-пошуковики (Startpage, Dogpile) дають більш широкий спектр результатів, а DuckDuckGo корисний для анонімного пошуку. Перевірка достовірності інформації вимагає зіставлення кількох незалежних джерел.

Додаток 5

РЕКОМЕНДАЦІЇ З ОСОБИСТОЇ БЕЗПЕКИ В ІНТЕРНЕТІ:

1. Завжди пам’ятайте про свою приватність. Не надавайте людям, з якими знайомитися, конфіденційну інформацію. Наприклад, в жодному разі не повідомляйте свої паспортні дані.
2. Перевірте людину у «чорних списках» аферистів — їх можна знайти у відкритому доступі в мережі. Наприклад, у фейсбуці чи на вебсайті «База шахраїв України».
3. Якщо людина, з якою ви спілкуєтеся на сайті знайомств, викликає у вас підозри чи дискомфорт, краще з самого початку припинити комунікацію з нею.
4. Намагайтеся поспілкуватися по відеозв’язку. Як правило, аферисти не бажають показувати власне обличчя, тому це чудова перевірка.
5. Якщо ви вирішили піти на побачення з людиною із сайту знайомств, обов’язково оберіть людне місце, яке ви добре знаєте, та заплануйте зустріч у денний час.
6. Повідомте людям, яким довіряєте, про місце зустрічі та надайте інформацію про людину, з якою йдете на це побачення. Якщо план раптово змінюється, то теж краще повідомити про це тих, кому довіряєте.
7. Якщо відчуваєте небезпеку, то одразу припиняйте зустріч та викликайте поліцію за номером 102.
8. Пам’ятайте, що людина, з якою ви спілкуєтеся в інтернеті, не завжди в реальному житті відповідає своєму віртуальному образу.
9. Перевіряйте покликання, які вам надсилає незнайома людина з інтернету. Вони можуть бути фішинговими. Наприклад, людина хоче отримати доступ до даних вашого профілю чи іншої інформації.
10. Не переказуйте гроші людині, з якою спілкуєтеся на сайтах знайомств. На жаль, аферисти та аферистки можуть вигадувати різноманітні історії (навіть дуже зворушливі та жалісливі), щоб отримати від жертв кошти.
11. Не варто надсилати свої інтимні фото навіть тій людині, яка викликає у вас симпатію і не є схожою на зловмисника. Так ви зможете уникнути шантажу і купи неприємностей у майбутньому.
12. Якщо вам не хочеться спілкуватися, йти на побачення чи робити будь-які інші дії з людиною із сайту знайомств, не робіть цього. Не варто силувати та ламати себе. Прислухайтеся до себе і своїх відчуттів.

КОНТАКТИ ДЛЯ ДОПОМОГИ, ЯКЩО ВИ СТРАЖДАЄТЕ ВІД НАСИЛЬСТВА В ІНТЕРНЕТІ:

Національна гаряча лінія для дітей та молоді - 0800500225 або 116111 (безкоштовно з усіх мобільних) чи в Telegram-chat – @CHL116111 або Instagram Direct – @childhotline_ua.

Єдиний контакт-центр системи безоплатної правової допомоги - 0800213103.

Уповноважений ВРУ з прав людини - 0800501720.

Сайт освітнього омбудсмена України.

Кіберполіція – 0800505170.

Урядова консультаційна лінія з питань безпеки в інтернеті – 1545*3.

Бот про безпечну поведінку в інтернеті – @StopSextingBot.

Чатбот «Кіберпес» для боротьби з кібербулінгом (у Viber).

Чатбот «Кіберпес» для боротьби з кібербулінгом (у Telegram).

Корисні джерела для самонавчання:

Інформаційно-освітня кампанія #stop_sextинг.

1. Стаття «Кібербулінг – що це та як це зупинити?».

2. Наказ Міністерства освіти і науки України «Деякі питання реагування на випадки булінгу (цькування) та застосування заходів виховного впливу в закладах освіти».

3. Стаття «Кібербулінг та кібергрумінг: поняття, протидія, відповідальність»;

4. Дія. Освіта. Кібербезпека.

5. Дія. Освіта. Освітній серіал «Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак».

6. DocuDaysUA. Кампанія проти кібербулінгу.

Для нотаток

Навчальне видання

Синиціна Юлія Петрівна

ОСНОВИ КІБЕРГІГІЄНИ

Методичні рекомендації
для підготовки до практичних занять

Редактор, оригінал-макет, дизайн –
А. В. Самотуга, О. М. Врублевська

Підп. до друку 27.05.2026. Формат 60х84/16. Друк – цифровий.
Гарнітура – Times New Roman. Ум.-друк. арк. 3,26. Обл.-вид. арк. 3,50.

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, т. (056) 370-96-59
Свідоцтво про внесення до державного реєстру ДК № 8112 від 13.06.2024 р.