

КІБЕРГІГІЄНА ТА ЦИФРОВА ГРАМОТНІСТЬ ЯК ОСНОВА БЕЗПЕКИ У МАЙБУТНЬОМУ РОЗВИТКУ УКРАЇНИ

Ковальчук Д. А.

*здобувач вищої освіти третього (освітньо-наукового рівня)
за спеціальністю 125 Кібербезпека
Міжнародний гуманітарний університет
м. Одеса, Україна*

Сучасний світ стає дедалі більш цифровим, і Україна активно рухається в напрямку цифрової трансформації. Проте зростання використання інформаційних технологій супроводжується підвищенням кіберзагроз, що ставлять під удар як окремих громадян, так і державні структури та бізнес. Атаки на банківські системи, державні реєстри, персональні акаунти громадян, маніпуляції через соціальні мережі та масові фішингові кампанії стали звичайним явищем.

Одним із головних способів зниження ризиків у кіберпросторі є формування культури кібергігієни та підвищення рівня цифрової грамотності населення. Кібергігієна – це комплекс заходів, які дозволяють користувачам безпечно взаємодіяти з цифровими технологіями, захищати свої персональні дані та уникати потенційних загроз.

Мета цієї роботи – проаналізувати сучасний стан цифрової грамотності в Україні, визначити основні виклики, що стоять перед громадянами та організаціями, а також запропонувати ефективні стратегії впровадження кібергігієни в суспільстві.

Завдання дослідження:

1. Окреслити поняття кібергігієни та цифрової грамотності.
2. Визначити основні загрози, що виникають через низький рівень кіберсвідомості.
3. Дослідити міжнародний досвід у сфері цифрової освіти.
4. Запропонувати практичні рекомендації для громадян, бізнесу та держави щодо підвищення цифрової безпеки.

Забезпечення цифрової грамотності та кібергігієни є не лише особистою відповідальністю кожного громадянина, а й важливим фактором національної безпеки, що сприятиме сталому розвитку України в умовах сучасних кіберзагроз.

Визначення кібергігієни та цифрової грамотності

Кібергігієна – це сукупність правил та практик, спрямованих на захист інформаційних систем, персональних даних та цифрових ресурсів

користувача. Подібно до особистої гігієни, вона вимагає регулярних дій, що мінімізують ризики цифрових загроз.

Цифрова грамотність, у свою чергу, охоплює не лише безпечне користування цифровими технологіями, а й уміння критично оцінювати інформацію, захищати свої дані та усвідомлювати потенційні загрози в кіберпросторі. Високий рівень цифрової грамотності є основою для ефективного впровадження кібергігієни.

Основні компоненти кібергігієни

Забезпечення кібергігієни вимагає дотримання певних принципів та правил. Основними з них є:

- **Використання надійних паролів** – застосування унікальних та складних паролів, використання менеджерів паролів.
- **Багатофакторна автентифікація (MFA)** – додатковий рівень захисту для облікових записів.
- **Оновлення програмного забезпечення** – регулярне встановлення оновлень для операційних систем та програм.
- **Обережність у соціальних мережах** – контроль за публічною інформацією, розпізнавання фейкових акаунтів.
- **Захист електронної пошти** – ідентифікація фішингових атак, уникнення підозрілих посилань та вкладень.
- **Безпечне користування публічним Wi-Fi** – використання VPN при підключенні до відкритих мереж.
- **Резервне копіювання даних** – регулярне створення резервних копій важливої інформації.

Основні компоненти цифрової грамотності

Цифрова грамотність охоплює ширший спектр компетенцій, які виходять за межі кібергігієни. До них належать:

- **Розпізнавання дезінформації** – вміння аналізувати інформацію та перевіряти її достовірність.
- **Розуміння принципів роботи алгоритмів соцмереж** – усвідомлення, як формуються стрічки новин і на що вони впливають.
- **Знання про персональні дані** – які дані збирають онлайн-сервіси та як їх обмежити.
- **Основи кіберетики** – правильна поведінка в цифровому середовищі, уникнення кібербулінгу.
- **Здатність працювати з цифровими сервісами** – онлайн-банкінг, електронний документообіг, цифрові ідентифікатори.

Формування культури кібергігієни та цифрової грамотності є критично важливим у сучасному суспільстві, оскільки нехтування цими аспектами може призвести до втрати даних, фінансових збитків та навіть загроз національній безпеці.

Основні кіберзагрози в Україні та світі

З розвитком цифрових технологій кіберзлочинці застосовують дедалі складніші методи атак, що загрожують не лише окремим користувачам, а й бізнесу, державним установам та критичній інфраструктурі. Найпоширенішими кіберзагрозами є:

- **Фішингові атаки** – зловмисники надсилають електронні листи або повідомлення, що імітують офіційні ресурси, щоб викрасти персональні дані.

- **Шкідливе програмне забезпечення (малваре, віруси, трояни, рансомваре)** – програми, що крадуть дані або блокують доступ до інформації з вимогою викупу.

- **Соціальна інженерія** – маніпулювання людьми з метою отримання конфіденційної інформації (наприклад, телефонні шахраї, які представляються співробітниками банку).

- **Витік персональних даних** – хакери викрадають дані користувачів з онлайн-сервісів або через слабкі паролі.

- **DDoS-атаки** – масовані запити до серверів, що спричиняють збої у роботі вебресурсів та онлайн-сервісів.

- **Атаки на мобільні пристрої** – шкідливі додатки, перехоплення повідомлень та дзвінків, використання заражених смартфонів для атак на інші системи.

Наслідки нехтування кібергігієною

Ігнорування правил кібербезпеки може мати серйозні наслідки як для окремих осіб, так і для держави загалом.

Для громадян:

- Викрадення персональних даних, що може призвести до фінансових втрат, шантажу або несанкціонованого доступу до облікових записів.

- Втрата коштів через шахрайські схеми (наприклад, зламани банківські акаунти).

- Поширення шкідливого програмного забезпечення через власні пристрої.

Для бізнесу:

- Злами корпоративних систем, що ведуть до витоку конфіденційних даних клієнтів та фінансових втрат.

- Репутаційні ризики – втрата довіри клієнтів через кібератаки або витоки даних.

- Вимагання викупу за заблоковані дані у разі атак типу рансомваре.

Для держави:

- Атаки на критичну інфраструктуру (енергосистеми, банківські установи, медичні та державні сервіси).

- Використання цифрових технологій для поширення дезінформації, що загрожуює національній безпеці.

- Зниження довіри громадян до цифрових сервісів та державних онлайн-платформ.

Проблема нехтування кібергігієною в Україні є особливо актуальною в умовах кіберконфліктів, де інформаційна безпека відіграє ключову роль у забезпеченні стабільності держави.

Стратегії та методи підвищення цифрової грамотності

Підвищення рівня цифрової грамотності є ключовим фактором у забезпеченні кібербезпеки населення та держави. Основні стратегії включають:

- **Освітні ініціативи** – впровадження курсів з кібергігієни в шкільну та університетську освіту, розробка навчальних матеріалів для дорослих.

- **Державні програми** – створення національних кампаній із цифрової безпеки, популяризація використання багатофакторної автентифікації та надійних паролів.

- **Роль бізнесу** – обов'язкове навчання працівників основам кібербезпеки, впровадження політик цифрового захисту в компаніях.

- **Міжнародний досвід** – адаптація успішних моделей цифрової освіти (наприклад, програми ЄС та США) для українських реалій.

Практичні рекомендації для громадян та бізнесу

Для ефективного підвищення кібергігієни необхідно:

Громадянам:

- Використовувати складні паролі та двофакторну автентифікацію.
- Бути обережними з електронною поштою та підозрілими посиланнями.

- Оновлювати ПЗ та робити резервні копії важливих даних.

Бізнесу:

- Запровадити навчання з кібербезпеки для співробітників.
- Використовувати корпоративні політики доступу до даних.
- Регулярно перевіряти безпеку інформаційних систем.

Висновки та перспективи. Підвищення цифрової грамотності та впровадження кібергігієни є критично важливими для безпечного розвитку України. Від цього залежить не лише безпека окремих користувачів, а й стійкість державних інституцій та бізнесу до сучасних кіберзагроз. Спільні зусилля держави, освітніх установ та приватного сектору допоможуть створити надійний цифровий простір та мінімізувати ризики інформаційних атак у майбутньому.