Горенчук Євгенія Андріївна
Студентка н.гр. 103_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

ОСНОВИ ЦИФРОВОЇ ГІГІЄНИ ДЛЯ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ

Сучасний світ неможливо уявити без інформаційних технологій. Працівники правоохоронних органів щодня використовують комп'ютери, мобільні пристрої, інформаційні бази даних і мережеві ресурси. У цих умовах питання цифрової гігієни – грамотного, безпечного та відповідального користування цифровими засобами, набуває особливої ваги.

Недотримання базових правил інформаційної безпеки може призвести до витоку службової інформації, зламу електронної пошти чи службових акаунтів, підробки документів або навіть кібератак на державні системи. Саме тому тематика цифрової гігієни є надзвичайно актуальною для підготовки майбутніх фахівців у сфері правоохоронної діяльності.

У сучасному світі розвиток інформаційних технологій суттєво впливає на діяльність правоохоронних органів. Більшість службових завдань пов'язана з використанням комп'ютерних систем, баз даних, електронного документообігу та мережевої взаємодії. У таких умовах важливого значення набуває поняття цифрової гігієни – сукупності правил, що забезпечують безпечне, відповідальне та ефективне користування інформаційними технологіями.

Цифрова гігієна – це система знань, навичок і звичок, спрямованих на захист користувача від кіберзагроз, витоку інформації та технічних збоїв.

Для працівників правоохоронних органів вона має особливе значення, оскільки недотримання базових правил може призвести до втрати службової інформації або порушення державної таємниці.

Основними принципами цифрової гігієни є:

1. Використання складних паролів та багатофакторної автентифікації.
2. Регулярне оновлення програмного забезпечення.
3. Заборона відкриття підозрілих електронних листів і посилань.
4. Використання офіційних джерел під час завантаження програм.
5. Захист персональних та службових даних від стороннього доступу.

6. Контроль конфіденційності у соціальних мережах.

Загрози у сфері цифрової безпеки правоохоронців.

Працівники правоохоронних органів часто стають мішенню кіберзлочинців, які намагаються отримати доступ до внутрішніх баз даних або персональних акаунтів. Найпоширеніші загрози: фішинг, шкідливе програмне забезпечення, злами месенджерів, соціальна інженерія. Важливо вміти розпізнавати ознаки кібератак і своєчасно повідомляти відповідні правоохоронни органи про підозрілі інциденти.

Правові аспекти цифрової гігієни.

В Україні питання кібербезпеки регулюються Законом України «Про основні засади забезпечення кібербезпеки» [1] та Законом України «Про захист персональних даних» [2]. Працівники правоохоронних органів зобов'язані дотримуватись вимог цих законів, не допускаючи розголошення службової або конфіденційної інформації у цифровому середовищі.

Отже, цифрова гігієна є невід'ємною частиною професійної культури правоохоронця. Вона сприяє збереженню особистої та службової інформації, підвищує рівень довіри громадян до поліції й державних інституцій загалом. Формування навичок цифрової грамотності – це запорука ефективної роботи в умовах сучасних кіберзагроз.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

2. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.