

3. Вишня В. Б. Інформаційні технології: навч. підручник. / В. Б. Вишня, К. Ю. Ісмаїлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : ДДУВС, 2020. 418 с.

4. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності: навч. посіб. Дніпро : ДДУВС, 2018. 218 с.

5. Вишня В. Б. Удосконалення системи управління нарядами мобільної патрульної служби Національної поліції України. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 2. С. 113-116.

***Ігонін Олександр Євгенович**
слухач магістратури НАВС*

Науковий керівник:

***Школьніков Владислав Ігорович**
доктор філософії, старший викладач
кафедри інформаційних технологій та
кібербезпеки ННІ №1 НАВС, капітан
поліції*

БЕЗПЕКА КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

Першим і найважливішим кроком до забезпечення безпеки вашої електронної скриньки є створення міцного пароля. Безпека починається зі створення надійного пароля. Надійний пароль – це пароль, який:

- Щонайменше 12 символів, але краще 14 символів.
- Комбінація букв у верхньому регістрі, букв нижнього регістра, чисел і символів.
- Це не слово, яке можна знайти у словнику або ім'я особи, символу, продукту чи організації.
- Значно відрізняється від попередніх.

Легко запам'ятати вас, але іншим користувачам складно вгадати. Рекомендовано використовувати таку пам'ятну фразу, як "6MonkeysRLooking^". Створивши надійний пароль, дотримуйтеся наведених нижче рекомендацій, щоб захистити його.

- Нікому не передавайте пароль. Це стосується навіть друзів і членів сім'ї.
- Ніколи не надсилайте пароль електронною поштою, у миттєвому повідомленні або за допомогою інших засобів зв'язку, які не гарантують надійного захисту.

- Використовуйте унікальний пароль для кожного веб-сайту. Якщо краде відомості облікового запису з одного сайту, вони намагатимуться використувати ці облікові дані на сотнях інших відомих веб-сайтів, таких як банківські послуги, соціальні мережі або покупки в Інтернеті, сподіваючись, що пароль повторно використовується в іншому місці. Це називається "Атака, яка має облікові дані", і вона дуже поширена.

- Якщо ви не хочете запам'ятовувати декілька паролів, скористайтеся диспетчером паролів. Найкращі диспетчери паролів будуть автоматично оновлювати збережені паролі, зберігати їх у зашифрованому вигляді та вимагати багатофакторну автентифікацію для отримання доступу.

- Поки ви їх захистите, ви можете записати паролі. Не пишіть їх на наліпках або картках біля тієї, яку захищає пароль, навіть якщо ви вважаєте, що вони добре приховані.

- Увімкніть багатофакторну автентифікацію за наявності. Для входу до облікового запису багатофакількома типами облікових даних, наприклад для введення пароля та одноразового коду, створеного програмою. Це додає ще один рівень безпеки на випадок, якщо хтось вгадає або викраде пароль.

Злочинці можуть спробувати зламати пароль, але іноді простіше скористатися слабкостями людини і виманити його в неї. Якщо ви отримали повідомлення електронної пошти від інтернет-магазину (наприклад, eBay або Amazon) або телефонний виклик від «банку», який намагатиметься переконати вас про «законне» отримання пароля або іншої важливої інформації, це може бути фішингове повідомлення.

Карпенко Анна Миколаївна
курсант 204 навчальної групи
ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший
викладач кафедри інформаційних технологій
та кібербезпеки ННІ № 1 НАВС, капітан
поліції

РОЛЬ СУЧАСНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ІНФОРМАЦІЇ

В сучасному світі, де цифрові технології проникають у всі сфери життя, питання безпеки інформації стає все більш актуальним. З кожним днем зростає кількість кіберзлочинів, загрози кібератак та порушень приватності.