

подальшого вдосконалення шляхом внесення змін до кримінального процесуального законодавства.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України: кодекс від 13.04.2012, редакція від 27.03.2022. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#n1089> (дата звернення: 11.04.2022 р.)

2. І. Гловюк. Кримінальне провадження в умовах воєнного стану. URL: <https://www.hsa.org.ua/blog/kryminalne-provadhennya-v-umovah-voyennogo-stanu/> (дата звернення: 11.04.2022 р.)

ІНФОРМАЦІЙНА БЕЗПЕКА ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІ В УМОВАХ ВІЙНИ

ЄСЬКОВА Катерина

курсантка 1-го курсу факультету № 1 Криворізького навчально-наукового інституту Донецького державного університету внутрішніх справ,
рядова поліції
науковий керівник:

ПАВЛИШ Тетяна

доцентка кафедри спеціальних дисциплін та професійної підготовки факультету № 1 Криворізького навчально-наукового інституту Донецького державного університету внутрішніх справ, кандидат педагогічних наук

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1].

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [2].

Більш детальне формулювання інформаційної безпеки – це стан захисту інформаційних потреб окремих людей, суспільств і націй незалежно від того, чи існують внутрішні та зовнішні загрози інформації, її існуванню та постійному розвитку [3].

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації [4].

З розвитком Інтернету, з'явилася можливість використовувати всі його досягнення в різних його проявах. Одним з таких проявів стали соціальні мережі, які набули на сьогодні статусу невід'ємного атрибуту нашого життя. Представити сучасну людину без соціальних мереж просто неможливо. Спілкування, пошук інформації і друзів, обмін новинами, можливість слухати музику, дивитися відео і фотографії. Складно собі уявити, що колись люди могли обійтися без профілю в соціальній мережі [5].

Особливої уваги заслуговують соціальні мережі працівників Національної поліції України в умовах воєнного стану. Інформація, що міститься на персональних сторінках соціальних мереж працівників поліції, надає змогу ідентифікувати особу, місце роботи і перебування, оцінити політичні вподобання та особисті інтереси. Тому з метою особистої інформаційної безпеки слід закрити особисті профілі Facebook, Instagram. Прибрати із профілей соціальних мереж особисту інформацію, обмежити коментарі, обмежити доступ до вашої сторінки у настройках приватності, не

додавати без критичного аналізу профілю у друзі незнайомих людей, перевіряти облікові записи (акаунти) тих, хто хоче стати вашим другом.

Аккаунт Google можна «убезпечити шляхом використання багатофакторної автентифікації». Усі без винятку онлайн-ресурси (електронна пошта, хмарні сховища, соціальні мережі) дають користувачам змогу захистити свої облікові записи за двофакторної автентифікації [6, с.13].

Як багатофакторна автентифікація можуть використовуватися:

1. SMS-повідомлення з тимчасовим кодом, який приходить на телефон, зареєстрований у сервісі.

2. Спеціальні програми, які генерують одноразовий тимчасовий код, який користувачеві потрібно ввести після введення пароля. Прикладом програми для багатофакторної автентифікації є Google Authenticator.

Працівники Національної поліції України також можуть долучатися до вилучення неприємного і неприйняттого контенту в Інтернет-сервісі YouTube, TikTok, Telegram-каналах шляхом скарги на дану інформацію.

Таким чином, враховуючи загрози інформаційній безпеці особистості поліцейського, а саме: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову) [7], працівники Національної поліції України повинні дотримуватися правил інформаційної безпеки, описаних вище і правильно і вчасно оцінювати ризики, які виникають у інформаційному просторі, особливо під час воєнного стану.

Список використаних джерел:

1. Стратегія кібербезпеки України. URL: <https://nncit.wunu.edu.ua/strategiya-kiberbezpeki-ukrayini/> (дата звернення: 11.04.2022).
2. Термін «Інформаційна безпека». Термінологія законодавства. Верховна Рада України: [сайт]. URL. <https://zakon.rada.gov.ua/laws/term/11458> (дата звернення: 12.04.2022).
3. Інформаційна безпека. Визначення інформаційної безпеки. URL: <https://sites.google.com/site/informacijnabezpeka15/-ponatta-informacijnoie-bezpeki/viznacenna-informacijnoie-bezpeki> (дата звернення: 12.04.2022).
4. Захист інформації та інформаційна безпека. URL: <http://referat-ok.com.ua/work/zahist-informacii-ta-informacijna-be/> (дата звернення: 12.04.2022).
5. Соціальні мережі: різні аспекти впливу на людину. *Українське право*. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_berkiy_Social_networks_and_there_involves/ (дата звернення: 13.04.2022).
6. Глебова А.О., Пістряга Т.В., Чуткий С.І. Онлайн безпека. Навчально-методичний посібник. К.: Піксель, 2022. 76 с.
7. Інформаційна безпека особистості URL: <https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka> (дата звернення: 14.04.2022).