Як поліція використовує засоби комунікації

Патрульна поліція використовує радіозв'язок для передачі важливої інформації до чергової частини, вказівок про плани дій, звітів про зупинених осіб, спостережень та іншої релевантної інформації. Це є критичним для забезпечення безпеки поліцейських та негайної реакції на потенційні загрози. Також радіозв'язок дозволяє контролювати роботу інших підрозділів.

Вивчення та використання сучасних технологій в процесі підготовки майбутніх правоохоронців значно підвищить їхні фахові компетенції та підготовку до служби. Це дозволить більш ефективно протидіяти злочинності та забезпечувати громадську безпеку [2].

Отже, інтернет, радіо та інші засоби комунікації стали невід'ємною частиною нашого життя, комунікації між підрозділами поліції, або у військовий цілях. Ці засоби допомагають швидко навчити майбутнього поліцейського потрібним навичкам, та допомагають забезпечити безпеку поліцейським.

_____

1. Доктрина «зі стратегічних комунікацій» вкп 10-00(49).01;

2. Теза «Використання новітніх технологій для розвитку навичок у майбутніх правоохоронців» Біліченко В. В. У збірнику «innovations and prospects in modern science» 20-22 november 2023.

УДК 004.738.5
DOI: 10.31733/15-03-2024/2/377-378

Світлана ПІВОВАРОВА
курсант Сумської філії
Харківського національного
університету внутрішніх справ.

Світлана ВИГАНЯЙЛО
доцент кафедри соціально-економічних
дисциплін Сумської філії
Харківського національного
університету внутрішніх справ,
кандидат економічних наук, доцент

БЕЗПЕКА ТА ЗАХИСТ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Враховуючи тенденції розвитку інформаційних технологій, одним з найбільш актуальних напрямків є використання інформаційних систем, які можуть забезпечити цілеспрямовану діяльність державних установ, та об'єднують такі компоненти як інформацію, процедури, персонал, апаратне і програмне забезпечення, які об'єднуються регульованими взаємовідносинами для формування єдиного цілого та забезпечення його цілеспрямованої діяльності. Враховуючи вищесказане на перший план можна поставити стан захищеності інформаційних систем, інформаційну безпеку. Інформаційна безпека – представляє собою набір процедур та інструментів, які захищають інформацію від неправомірного використання, несанкціонованого доступу, псування або знищення. Як і будь-яка власність, інформація потребує захисту. Проблема захисту інформації повинна враховувати такий важливий аспект як захист права громадян на вільний доступ до відомостей, що гарантовано Конституцією України. Основи захисту інформації розробляються державними органами влади із врахуванням необхідності забезпечення інформаційної безпеки, зокрема національної безпеки України в цілому.

Інформаційна безпека забезпечується трьома напрямками: конфіденційності, цілісності та доступності.

Конфіденційність інформації – це гарантія, що дані доступні лише тим, кому це дозволено. Її можна досягти за допомогою: шифрування даних, а саме перетворення інформації на код, який можуть розшифрувати лише авторизовані користувачі; багатофакторної автентифікації – сукупність декількох методів підтвердження особистості користувача, таких як, пароль, код з SMS або відбиток пальця; захист від втрати даних

(несанкціонованого копіюванню, видалення або викрадення інформації).

Цілісність інформації досягається за рахунок підтримки та забезпечення точності і цілісності даних протягом всього життєвого циклу, що критично важливо при проектуванні, впровадженні та експлуатації систем, призначених для зберігання, обробки та постачання даних.

Доступність інформації полягає в тому, що користувач може використовувати цей ресурс згідно з правилами, встановленими політикою безпеки не очікуючи довше заданого інтервалу часу.

Для забезпечення інформаційної безпеки необхідно використовувати комплексний підхід, який охоплює всі три напрямки. Неможливо створити систему, захист якої не можна зламати, більш реальним може бути створення такого механізму захисту, вартість злому якого буде дорожчою за інформацію, яку можна отримати. Тому доцільним буде впровадження програмних засобів безпеки, які вмонтовані до складу програмного забезпечення системи і є потрібними для виконання функцій захисту.

Розглянемо принципи, що забезпечують інформаційну безпеку:

1. Законність (захист персональних даних; забезпечення правомірного доступу до інформації та її обробки; дотримання чинного законодавства України в сфері інформаційної безпеки).

2. Баланс інтересів особи, суспільства і держави (здійснення державного управління в інформаційній сфері; захист суспільства від інформаційних загроз; забезпечення інформаційних прав та свобод особи).

3. Комплексність (застосування сукупності організаційних, технічних та програмних заходів захисту інформації; врахування всіх напрямків інформаційної безпеки, включаючи конфіденційність, цілісність, доступність, незаперечність та підзвітність.)

4. Системність (постійне вдосконалення системи інформаційної безпеки; створення багаторівневої системи захисту інформації; забезпечення єдності та взаємозв'язку всіх компонентів системи інформаційної безпеки).

Саме через дотримання принципів інформаційної безпеки та впровадження комплексної та превентивної стратегії захисту інформаційних систем досягається мінімізація ризиків, пов'язаних з кібератаками, безперебійною роботою та збереженням конфіденційності інформації.

---

1. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації: Посібник для курсантів ВНЗ МВС України. Київ: Національна академії внутрішніх справ, 2012. 104с https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf (Дата звернення: 01.03.2024).

2. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 81/94 ВР. Дата оновлення: 16.12.2020. URL :https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (Дата звернення: 02.03.2024).