Наразі зазначимо, що функції держави включають у себе функцію захисту. Відтак, згідно ст. 17 Конституції України: «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [1].

Під інформаційною безпекою слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [2]. Відтак, інформаційна безпека – являє собою нерозривну дуже важливу систему захисту держави у сфері обігу інформації, наприклад (політичної інформації або військової інформації), а також захист від потенційних зовнішніх та внутрішніх загроз, які себе можуть проявляти, як у просторі Інтернету, так і на передовій фронту України.

Отже, погоджуємось зі словами О. Довгань, а саме, що для успішного входження нашої держави в міжнародний інформаційний обмін вона має зосередитись насамперед у сфері правової діяльності за такими напрямками: розробити, розвинути та ввести в дію систему нормативно-правових актів, спрямованих на високий рівень захисту національних інформаційних ресурсів використання в національних інтересах; створити законодавчу базу для регулювання участі в міжнародній діяльності для забезпечення дотримання міжнародного інформаційного законодавства, такого як боротьба з кібертероризмом. [3].

Отже, враховуючи все вищесказане та спираючись на те, що дана тематика потребує більшої уваги з боку науковців та правотворчих органів можна дійти до висновку, що інформаційна безпека в Україні, є важливою складовою національної безпеки. І вище перелічені напрямки вдосконалення законодавства, є не вичерпними для збільшення інформаційного захисту у державі. І на сьогодні варто приділяти значну увагу цьому питанню та переходити у наступальні дії, особливо у зв'язку з кібератаками та дезінформацією ворога на передовій.

1. Конституція України URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [дата звернення 26.02.2024]

2. Боднар, І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія. Львівської комерційної академії, 2013. 320 с.

3. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. *Правова інформатика. № 4(40)*. 2013. С. 79-88.

УДК 355.451
DOI: 10.31733/15-03-2024/2/375-377

Ілля ПАРФЬОНОВ
курсант факультету підготовки
фахівців для підрозділів
кримінальної поліції

Валерій БІЛІЧЕНКО
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

РОЛЬ ТА ЕФЕКТИВНІСТЬ СИСТЕМ КОМУНІКАЦІЙ ТА КООРДИНАЦІЇ У СПЕЦІАЛЬНИХ ВІЙСЬКОВИХ ПІДРОЗДІЛАХ: АНАЛІЗ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

У сучасній війні головне – швидкість та ефективність комунікації між підрозділами. Щоб ефективно вести війну, потрібно заохочувати інших громадян допомагати вести бойові дії – створювати речі, перевозити їжу, допомагати евакуювати цивільних людей з окупованих територій та інше.

Все це було б неможливо без сучасних методів комунікації. Потрібно швидко передавати інформацію, але так, щоб її не перехопив ворог. Для цього створили різні

методи шифрування. Радіо та інтернет – це повністю відкриті канали комунікації, тобто кожен може перехопити ваш сигнал та розшифрувати його.

Але використовують засоби комунікації не тільки військові, а ще й поліція, для ефективного здійснення своїх повноважень.

Інформаційне суспільство потребує фахівців, які вміють швидко адаптуватися до змін, здатні освоїти нові знання та оволодіти новими вміннями в короткі терміни [2].

Радіо

Радіомовлення надає кілька способів передачі інформації зашифрованою або так, щоб ворог не зміг зрозуміти:

1. Позивні: це псевдоніми підрозділів або осіб.
2. Ключові слова або фрази: ці фрази визначаються заздалегідь і розуміються тільки тими, хто домовився використовувати їх. Наприклад, «Медвідь в лісі» може означати «Танк в лісі».

Також можна використовувати цифрові методи шифрування, такі як SHA256. Цей метод працює наступним чином:

1. Пристрій вловлює звукові хвилі – мову.
2. За допомогою АЦП (Аналогового-Цифрового Перетворювача) звук перетворюється у числа, які представляють собою точки на графіку звукової хвилі.
3. Ці дані шифруються за допомогою алгоритму SHA256.
4. Зашифровані дані передаються по радіо.

Проблеми використання радіо

Радіо – це електромагнітна хвиля, яку можна заглушити за допомогою спеціальних пристроїв, або вона може стикатися з перешкодами через погодні умови (такі як туман, блискавка і т. д.). Проте, якщо перешкоди не є сильними, то при використанні цифрових радіостанцій сигнал може залишатися стійким.

Щодо передачі радіосигналу на великі відстані, необхідно враховувати наступне:

1. Чим вище розташований радіопередавач, тим далі можна передавати сигнал.
2. Збільшення потужності радіостанції також допомагає збільшити дальність передачі сигналу.
3. Використання цифрових методів передачі сигналу забезпечує кращу стійкість до перешкод та шуму.
4. Використання FM (частотної модуляції) також дозволяє ефективно передавати сигнал на великі відстані, оскільки цей тип модуляції має деякі переваги щодо шуму та перешкод.

Інтернет

Інтернет може бути використаний для передачі інформації для інформування населення, але через те, що інтернет є публічним, ворог може використовувати його для дезінформації вашого населення.

Для швидкої передачі інформації можна використовувати соціальні мережі. Проте, це не завжди безпечний спосіб, особливо якщо ви не маєте впевненості, що компанія, яка підтримує цю соціальну мережу, не передасть ключі та доступ ворогу, що може дозволити ворогові прочитати всі ваші повідомлення.

Інформування населення є теж дуже важливою складовою ведення війни. Для інформування населення зазвичай використовують такі веб-сайти, як YouTube, Facebook, Telegram, Instagram та інші.

У сучасний час використання газет для інформування населення вважається неефективним, адже майже ніхто не читає газети.

Проблеми використання інтернету

Для підключення до Інтернету потрібна послуга провайдера, який забезпечує доступ до мережі. Зазвичай для підключення до Інтернету використовуються цифрові радіолінії -мобільний зв’язок. Однак, у віддалених районах може бути важко отримати доступ до цих станцій.

У воєнний час зазвичай використовуються супутникові зв’язки, але це дуже дорогий спосіб зв’язку, і кількість станцій, які можуть підключитися до супутника обмежена.

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