система «Цунамі»).

1. Використання інформаційних технологій в діяльності Національної поліції України.URL: https://univd.edu.ua/science-issue/issue/379

2. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото і кінозйомки, відеозапису. Аналіз закордонного досвіду. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/5a48c83f-6d5b-4435-b9d4-0cbd34d42dc8/content ст. 35

3. Інформаційне забезпечення діяльності патрульної поліції. URL: http://surl.li/mzqmm

Ткаченко Павло Олександрович
аспірант кафедри
кримінально-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
член Асоціації правників України
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНАМИ ДЕРЖАВНОЇ БЕЗПЕКИ

У сучасному світі інформаційні технології відіграють ключову роль у всіх сферах суспільного життя. Цифрова трансформація спричинила значне збільшення обсягу інформації, яку обробляють. Від цього залежить успішність функціонування сучасних організацій та держав в цілому. Однак разом з розвитком інформаційних технологій зросли загрози для безпеки інформації. Тому останнє десятиріччя особливо актуальною стала проблема забезпечення інформаційної безпеки, зокрема органами державної безпеки.

Більшість теоретиків вважає, що забезпечення інформаційної безпеки органами державної безпеки – це система заходів та стратегій, спрямованих на запобігання несанкціонованому доступу, використанню, розголошенню чи пошкодженню інформації, яка є важливою для національних інтересів та безпеки країни.

Водночас, на нашу думку, забезпечення інформаційної безпеки органами державної безпеки полягає не лише в захисті інформації, як такої. У

складі ключового органу забезпечення державної безпеки країни – Служби безпеки України ефективно функціонує підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, який щоденно, щохвилинно здійснює захист інформаційних систем, електронних платформ державних органів від злочинних посягань, інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури від кібератак, здійснює контррозвідувальне та оперативне забезпечення всіх гілок держави, що в підсумку виражається в захищеності цих об'єктів від протиправних посягань.

Сьогодні рівень професіоналізму представників підрозділів КІБ СБУ знаходиться на найвищому рівні, адже фахівці саме цього, особливо важливого органу забезпечують інформаційну та кібернетичну безпеку Збройних Сил України, Національної гвардії України, Державної прикордонної служби України, Державної спеціальної служби транспорту України та інших військових формувань, які утворені відповідно до чинного законодавства України.

Забезпечують Збройні Сили України від перешкоджання законній діяльності останніх, виявляючи осіб та документуючи їх протиправну діяльність, притягують до кримінальної відповідальності.

Щодо загальної площини забезпечення інформаційної безпеки органами державної безпеки, то варто зауважити, що ця діяльність є надзвичайно важливим завданням в умовах сучасного цифрового суспільства, коли інформація стала ключовим активом для багатьох сфер діяльності, включно з обороною, економікою, наукою, політикою та громадським життям. Органи державної безпеки забезпечують захист інформації з обмеженим доступом від втрати, несанкціонованого доступу, розголошення чи пошкодження. Важливими аспектами забезпечення інформаційної безпеки органами державної безпеки є кібербезпека, сутність якої полягає в тому, що органи державної безпеки розробляють стратегії та заходи для захисту державних інформаційних систем від кіберзагроз. Це містить заходи щодо виявлення, запобігання та реагування на кібератаки, віруси, хакерські атаки та інші електронно-інформаційні загрози.

Правове регулювання полягає в розробці та впровадженні відповідного законодавства, яке регулює обіг та захист інформації. Організаційна безпека – розроблення політик, процедур та правил внутрішньої організації для забезпечення інформаційної безпеки в установі чи організації. Це містить навчання персоналу та формування безпекової культури в організації. Боротьба з дезінформацією та фейками повинна містити у собі розроблення стратегій та методів виявлення та запобігання поширенню дезінформації та фейків, особливо в соціальних мережах та медіа, що на сьогодні ефективно забезпечується саме підрозділами КІБ СБУ, під контролем яких перебувають всі соціальні мережі та інформаційні платформи.

Технічні заходи безпеки полягають в застосуванні технологічних засобів для забезпечення безпеки інформації, зокрема шифрування, використання

безпечного програмного забезпечення, мережеві заходи безпеки та інші технічні методи. Моніторинг та реагування ґрунтується на постійному моніторингу захищеності систем та інфраструктури для виявлення можливих атак та негайного реагування на них.

Отже, забезпечення інформаційної безпеки є актуальним завданням для органів державної безпеки в умовах сучасного цифрового світу. Швидкий та непередбачуваний розвиток інформаційних технологій відкриває безліч можливостей для збереження, обробки та передачі інформації, але водночас створює загрози для її конфіденційності та цілісності. Органи державної безпеки повинні вживати комплексних заходів для гарантування інформаційної безпеки.

Кібербезпека є основним компонентом забезпечення інформаційної безпеки. Захист інформаційних систем від кібератак, застосування сучасних технологій шифрування та виявлення загроз є невід'ємною частиною цього процесу. Важливо вдосконалювати та адаптувати кіберзахист відповідно до нових загроз та атак. Технічні засоби безпеки та організаційна безпека є важливими аспектами для захисту важливої інформації та уникнення загроз. Впровадження сучасних технологій та розробка ефективних процедур дозволяють убезпечити системи від несанкціонованого доступу та атак.

Інформаційна освіта та навчання мають ключове значення для підвищення рівня обізнаності населення та співробітників у сфері інформаційної безпеки. Вони дозволяють ефективно реагувати на загрози та уникати можливих негативних наслідків.

Усі ці компоненти повинні бути інтегровані в систему забезпечення інформаційної безпеки, яка повинна бути постійно оновлюваною та адаптованою до змін у технологічному та соціальному середовищі. Лише комплексний підхід та спільні зусилля можуть гарантувати ефективність заходів забезпечення інформаційної безпеки в умовах сучасного світу.