професійно-технічної освіти, незалежно від спеціальності, можуть і повинні враховувати це у своїй виховній роботі серед студентів, надаючи їм знання та засоби критичного мислення, раціоналізму та аналізу інформації. Окрім того, навчальні заклади можуть проводити лекції та семінари з інформаційної боротьби, запрошувати експертів для виступів з доповідями, організовувати круглі столи та дискусії [3, с. 236].

Зокрема, інформаційна діяльність може передбачати створення інформаційних матеріалів, що містять правдиву інформацію про події, що відбуваються в країні. Ці матеріали можна розміщувати на сайтах навчальних закладів та на їхніх сторінках у соціальних мережах, що дасть можливість охопити їх широку аудиторію. Ви також можете організовувати виставки, конференції та інші заходи для підвищення обізнаності про інформаційну війну.

1. Кулеба Д. Війна за реальність. *Як перемагати у світі фейків, правд і спільнот.* Вип. 1. 2022р., 384 с.

2. Мороз О. Боротьба за правду. *Як мій дядько переміг брехню.* Вип. 1. 2022р., 321 с.

3. Патрикаракос Д. Війна у 140 знаках. *Як соціальні медіа змінюють конфлікти у XXI столітті.* Вип. 1. 2023р., 337 с.

УДК 004.056.53:351.74
DOI: 10.31733/15-03-2024/2/380-382

Назарій РАБУШКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Юлія СИНИЦІНА
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗАПОБІГАННЯ ВНУТРІШНІМ ЗАГРОЗАМ ТА МОЖЛИВИМ СПРОБАМ НЕСАНКЦІОНОВАНОГО ДОСТУПУ АБО ВИТОКУ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Злочинність, як і всі інші сфери людської діяльності, постійно розвивається із застосуванням нових технологій, наукових, технічних розробок тощо, чим змушує правоохоронні органи, зокрема і Національну поліцію України впроваджувати відповідні контрзаходи з метою виконання покладених на неї повноважень. У реаліях сьогодення підрозділами Національної поліції України використовується 77 різноманітних інформаційних систем з обмеженим доступом. Це різноманітні системи які забезпечують професійну діяльність. Кількість цих систем може змінюватись в залежності від конкретних потреб і функцій, що виконуються. Наприклад, це можуть бути системи для обліку злочинів, бази даних з інформацією про підозрюваних або викрадені предмети, системи для спостереження за громадським порядком тощо.

Актуальність теми полягає в тому, що сучасна діяльність правоохоронних органів, зокрема поліції, все більше піддається впливу кіберзагроз та інших форм кіберпреступності. В умовах зростаючого використання цифрових технологій у роботі поліції, важливо забезпечити ефективний захист інформаційних ресурсів від потенційних загроз. Необхідно удосконалювати системи кібербезпеки, виявляти та запобігати внутрішнім загрозам, а також реагувати на можливі спроби несанкціонованого доступу або витоку конфіденційної інформації. Захист інформаційної безпеки Національної поліції має вирішальне значення для збереження довіри громадськості, забезпечення правопорядку та успішного виконання службових обов'язків.

Із метою організації інформаційно-аналітичного забезпечення поліції було розроблено Положення про інформаційно-телекомунікаційна систему «Інформаційний

портал Національної поліції України». Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі – система ІПНП) – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення [1].

Але іноді трапляються випадки так званого витоку інформації, тобто момент коли доступ до неї отримує не уповноважена на це особа. Такі витоки можуть загрожувати безпеці громадян, суспільства і держави.

В свою чергу ми пропонуємо наступні заходи запобігання витоку інформації в діяльності Національної поліції:

1. Зміцнення культури конфіденційності: налагодження системи освіти та навчання для поліцейських про конфіденційність і захист конфіденційної інформації.
2. Регулярні аудити та перевірки безпеки: проведення регулярних перевірок та аудитів систем безпеки інформації для виявлення потенційних слабких місць та вразливостей.
3. Захист доступу до інформації: обмеження доступу до конфіденційної інформації лише для авторизованих осіб та встановлення системи контролю доступу.
4. Шифрування даних: застосування шифрування для захисту конфіденційної інформації під час передачі та зберігання.
5. Суворі дисциплінарні заходи: встановлення чітких правил та процедур для використання та обробки конфіденційної інформації, а також накладання суворих дисциплінарних заходів за порушення цих правил.
6. Підвищення свідомості персоналу: проведення навчань та інформаційних кампаній для персоналу щодо ризиків витоку інформації та методів її запобігання.
7. Захист фізичних засобів: забезпечення безпеки фізичних засобів, таких як комп'ютери, сервери та документи, що містять конфіденційну інформацію. Для прикладу, як зазначають автори Краснобрижий І.В., Прокопов С.О., Рижков Е.В. та Синиціна Ю.П.: «Використання незахищених оболонок може призвести та вже призводило до витоку службової інформації» [2, 3], а тому необхідно використовувати спеціально призначені для цього технічні системи.
8. Співпраця з іншими службами безпеки: Розвиток співпраці з іншими правоохоронними та розвідувальними органами для обміну інформацією та спільної боротьби з витоками.

До основних перспективних напрямків можна віднести наступні:

1. Розробка та впровадження програм та стратегій кібербезпеки для Національної поліції, спрямованих на запобігання внутрішнім загрозам та захист інформаційних ресурсів.
2. Підвищення кваліфікації та навичок персоналу Національної поліції у сфері кібербезпеки, зокрема навчання та тренінги з профілактики та реагування на можливі кібератаки.
3. Розвиток спеціалізованих підрозділів або центрів кібербезпеки в Національній поліції для виявлення, аналізу та відповіді на потенційні загрози та інциденти кібербезпеки.
4. Запровадження систем моніторингу та аналізу внутрішньої діяльності та доступу до інформації в Національній поліції з метою виявлення та запобігання несанкціонованому доступу або витоку інформації.
5. Удосконалення законодавства та правил внутрішньої поліцейської діяльності з урахуванням сучасних кіберзагроз та вимог кібербезпеки.

Також під особливо жорсткий контроль необхідно взяти медіа, соцмережі та окремих громадян, які фіксують та публікують ті чи інші події пов'язані з веденням бойових дій, ракетних, дронових влучать, тощо. Такі події неможливо назвати несанкціонованим доступом або витоком інформації, оскільки хронологічно вона опиняється у поліції у другу чергу. Поліція в свою чергу повинна проводити профілактичні заходи щодо нерозповсюдження даного виду інформації, впливаючи на свідомість людей та притягуючи до відповідальності згідно з законом.

На сьогоднішній день, використання системи інформаційного порталу Національної поліції довело свою ефективність, навіть враховуючи можливі ризики несанкціонованого доступу чи витоку інформації. Оскільки негативні наслідки неможливо прорахувати навіть приблизно, а тому необхідно запобігати несанкціонованому доступу або витокам інформації, що використовується в діяльності Національної поліції. Зокрема варто зазначити, що в умовах воєнного стану дана тема набуває особливої актуальності, оскільки

ворогу важливо знати інформацію, яку він зможе використовувати для тероризування населення та проведення ІПСО компанії.

У зв'язку з постійним розвитком технологій та зростаючою загрозою кіберпреступності, Національна поліція України змушена впроваджувати нові контрзаходи для захисту інформаційних ресурсів та виконання своїх функцій. У цьому контексті актуально вдосконалювати системи кібербезпеки та запобігати внутрішнім загрозам та можливим витокам інформації. Важливо, також постійно вдосконалювати інформаційні системи з обмеженим доступом та забезпечувати їх ефективність.

Профілактика витоку інформації в діяльності Національної поліції вимагає комплексного підходу та застосування різноманітних заходів. Крім того, важливо співпрацювати з іншими службами безпеки, проводити навчання персоналу щодо ризиків витоку інформації та розвивати спеціалізовані підрозділи кібербезпеки.

1. Наказ МВС «Про затвердження Положення про інформаційно телекомунікаційну систему «Інформаційний портал Національної поліції України» від 3.08.2017 № 676.

2. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності: навч. Посіб. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. 218 с.

3. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка: навч. посіб.. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2022. 244 с.

УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/382-383

Анастасія САВЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Віктор БОГУСЛАВСЬКИЙ
завідувач кафедри кафедри
спеціальної фізичної підготовки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ОСНОВНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Динамічний розвиток процесів цифровізації відкрив нові можливості, але й став джерелом ризиків і загроз для національної економіки, зокрема для інформаційної безпеки. Поза традиційними загрозами, такими як промислове шпигунство, ненавмисне розголошення конфіденційної інформації або комерційної таємниці, дії недобросовісних конкурентів та втручання сторонніх осіб у інформаційні системи і мережі, існують і додаткові загрози для інформаційних ресурсів і технологій в економіці.

До них відносяться кібератаки, розкриття персональних даних, вплив шпигунських програм і вірусів, фішинг, загрози, пов'язані з оновленням комп'ютерних програм тощо. Методи діагностики і протидії цим загрозам поки не повністю вивчені [1, с.34].

Моніторинг рівня кібербезпеки України та визначення шляхів розбудови національної системи кіберзахисту, а також висвітлення основних проблем і напрямків їх вирішення, стають все більш важливими в умовах постійного зростання кіберризиків і кіберзагроз.

Кібербезпека України забезпечується через виконання збалансованої державної політики відповідно до прийнятих у встановленому порядку доктрин, концепцій, стратегій і програм. Основними напрямами державної політики у сфері кібербезпеки України є [3]:

- Створення захищеного національного сегмента кіберпростору, сприяючи підтримці відкритого суспільства та забезпечуючи безпечне використання цього простору суспільством.