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.

- Запобігання втручанню у внутрішні справи України та нейтралізація посягань на її інформаційні ресурси з боку інших держав.
- Посилення обороноздатності держави у кіберпросторі.
- Боротьба з кіберзлочинністю та кібертероризмом.
- Зниження рівня уразливості об'єктів кіберзахисту.
- Забезпечення повноправної участі України в загальноєвропейських і регіональних системах забезпечення кібербезпеки.
- Дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом.

Вибір конкретних заходів і шляхів забезпечення кібербезпеки України зумовлюється необхідністю своєчасного вжиття заходів, що адекватні характеру та масштабам реальних і потенційних кіберзагроз життєво важливим інтересам людини та громадянина, суспільства і держави.

Розвиток міжнародної співпраці для посилення кіберстійкості України стає пріоритетним завданням у зусиллях попередження глобальних інформаційних загроз, забезпечення якості розслідування кіберзлочинів, затримання та переслідування зловмисних агентів, а також подолання проблем кібербезпеки.

Варто відзначити, що існують напрями у сфері кібербезпеки, які негативно впливають на позиції України та вимагають вдосконалення. Зокрема, це низький рівень внеску в глобальну кібербезпеку, недостатній рівень захисту цифрових послуг та недостатньо розвинений напрям військових кібероперацій.

Наприкінці 2022 року Україна активно долучилася до міжнародного співробітництва у сфері кібербезпеки, і проводиться процес формування кібервійська, відповідального за інформаційну безпеку, захист критичної інфраструктури та розвідку [2]. Враховуючи досягнення України в кіберпросторі, обґрунтовано визнати її рівноправним учасником на міжнародній арені у сфері кібербезпеки.

Загалом, варто зауважити про те, що серед перспективних завдань є подальше удосконалення систем інформаційного захисту об'єктів критичної інфраструктури на основі передових світових практик та узгодженість дій з міжнародними організаціями щодо протидії загрозам, пов'язаним з розвитком цифрової економіки та інформаційного суспільства. Побудова ефективної системи кібербезпеки сприятиме формуванню превентивного механізму протидії загрозам та їх стримуванню, а також випереджальному реагуванню на динамічні зміни у кіберпросторі.

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. Відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. Київ. 2023. №7 (липень) . 270 с.

2. Microsoft Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. April 27, 2022.

3. Основні напрями забезпечення кібербезпеки України. URL : https://core.ac.uk/download/pdf/84825452.pdf