Тарасенко Олег Сергійович,
доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Кримський Тарас Святославович,
аспірант наукової лабораторії з проблем протидії злочинності Національної академії внутрішніх справ

ОСНОВНІ ЦІЛІ ТА ЗАВДАННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ НА 2021-2025 РОКИ

Характерною ознакою сучасного світу стало масове й стрімке впровадження цифрових інформаційних технологій у різні сфери суспільної діяльності. Державне управління, медицина, наука, військова сфера, правоохоронна діяльність, товарне виробництво, зв'язок – все перейшло на електронний документообіг, цифрову обробку, збереження та використання інформації.

У даний непростий час для українського суспільства, в тому числі враховуючи збройну агресію іноземних держав щодо України, вкрай важливим є захист її кіберпростору та інформаційної безпеки.

У зв'язку з цим Радою національної безпеки і оборони України розроблено проект Стратегії кібербезпеки України (2021-2025 роки) (далі – Стратегія) [1].

Стратегією передбачено, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Окрім цього, нові виклики несе з собою перехід на 5G-мережі, функціонування яких кардинальним чином залежить від коректної роботи програмного забезпечення, що за рахунок новизни технології може мати нові, не повною мірою передбачені загрози. Технології «Інтернет речей», «розширена реальність», «розумне місто» активно доповнюються новими – «гіперавтоматизація», «розумно

компонований бізнес», «кібербезпекова сітка», «розподілена хмара», «Інтернет-поведінка» тощо.

Докорінно змінюючи світовий життєустрій, пандемія коронавірусу COVID-19 матиме довготривалий вплив на світовий порядок. Зростає залежність від цифрових комунікацій, що робить вразливим процес обміну інформацією, захисту інформації та персональних даних. Кіберзлочинці, максимально використовуючи тему пандемії, від її початку все більше застосовують нові методи проведення кібератак, що змушує національні уряди впроваджувати додаткові механізми протидії, збереження доступу до необхідних пристроїв, належного функціонування всіх потрібних для життя та роботи електронних ресурсів і систем.

На сьогоднішній день можна стверджувати, що надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії кібербезпеки України Затвердженої Указом Президента України від 15 березня 2016 року № 96/2016 [2] не були виконані: не сформовано перелік критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично.

Новою стратегією передбачено наступні стратегічні цілі, а саме: дієва кібероборона, посилення спроможностей у протидії розвідувальнопідривній діяльності у кіберпросторі та кібертероризму, посилення спроможностей у протидії кіберзлочинності, розвиток асиметричних інструментів стримування, посилення національної кіберготовності та кіберзахист, професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки, безпечні цифрові послуги, зміцнення системи координації, формування нової моделі відносин у сфері кібербезпеки, прагматичне міжнародне співробітництво.

Стратегією запропоновано проведення аудиту імплементації в українське законодавство положень Конвенції про кіберзлочинність [3] та завершення цього процесу шляхом внесення необхідних змін до законів України та врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики та підхід країн-членів ЄС з цих питань.

Врегулювання проблем використання електронних доказів у сьогоденні є надзвичайно важливим для правоохоронних органів України, яке допоможе швидко та якісно збирати і використовувати докази у кримінально – процесуальному судочинстві.

В Україні буде проведено наукові дослідження у сфері кібербезпеки, реформовано систему підготовки та підвищення

кваліфікації кадрів, а також розгорнуто навчальні програми, курси, тренінги з кібернавчання для всіх верств населення. У зв'язку з тим, що життєдіяльність населення з кожним роком все більше переходить в інформаційний простір, підвищення кваліфікації всіх верств населення сприятиме пришвидшенню даних процесів життєдіяльності.

Не менш важливим питанням є впроваджування цифрових послуг для населення та розвиваток національної інформаційної інфраструктури, передбачаючи виділення коштів на заходи кібербезпеки та кіберзахисту в розмірі не менше ніж 5% від загальної вартості відповідного об'єкта інформаційної інфраструктури (інформаційно-комунікаційної системи).

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Як загальний висновок, необхідно зазначити, що проект Стратегії кібербезпеки України (2021-2025 року) передбачає впровадження ряду необхідних завдань та цілей спрямованих на ефективне забезпечення кібербезпеки України. Подальшим кроком повинно бути забезпечено впровадження даних завдань та цілей в життєдіяльність України, а не залишення їх тільки «на папері».

Список використаних джерел

1. Проект Стратегії кібербезпеки України (2021-2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016. *URL:* https://zakon.rada.gov.ua/laws/show/96/2016#Text;

3. Конвенція про кіберзлочинність від 10.09.2007. 2007. № 65. С. 107. Ст. 2535. *URL*: https://zakon.rada.gov.ua/laws/show/994_575#Text.