тварин;

4) надання спільної допомоги населенню внаслідок надзвичайних ситуацій природнього та техногенного характеру, боротьба з наслідками від них;

5) надання безоплатної гуманітарної допомоги, в т.ч. з-закордону товарів для військових за декларативним принципом;

6) забезпечення технічним обладнанням, одягом, бронежилетами, автівками тощо.

7) забезпечення міжнародної комунікації.

Література

1. Про волонтерську діяльність: Закон України від 19 квіт. 2011 р. № 3236-VI. Відомості Верховної Ради України. 2011. № 42. Ст. 435.

2. Про державний захист працівників суду і правоохоронних органів: Закон України від 23 груд. 1993 р. № 3781-XII. Відомості Верховної Ради України. 1994. № 11. Ст. 50.

УДК 342.951:351.82 + 32.019.51(043.2)

Криволап Є.В., здобувач вищої освіти
третього (освітньо-наукового) рівня,
Національний авіаційний університет, м. Київ, Україна

ВПЛИВ СТРАТЕГІЙ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЗПЕКИ НА ІНШІ БЕЗПЕКОВІ СТРАТЕГІЇ УКРАЇНИ

Розглядаються окремі питання впливу Стратегій інформаційної та кібербзпеки на інші безпекові стратегії України. Звертається увага, що протягом 2020-2021 рр. доктринальні положення щодо державної безпеки України у різних галузях державного і суспільного життя знайшли радикальне оновлення. Оскільки сфера інформаційної безпеки та кібербезпеки є сферою активного протиборства [1 та ін.], особливо в умовах агресивних дій російської федерації (рф) проти України, то дослідження поставленого питання є актуальним.

Згідно ч. 1 ст. 4 Закону України від 21.06.2018 року № 2469-VIII «Про національну безпеку України», державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, ***інформаційної***, екологічної безпеки, безпеки критичної інфраструктури, ***кібербезпеки*** України та на інші її напрями.

У пункті 45 Стратегії національної безпеки України пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції визначені: активна та

ефективна протидія розвідувально-підривній діяльності, спеціальним ***інформаційним операціям та кібератакам***, російській та іншій підривній пропаганді.

Серед викликів і загроз у сфері інформаційної безпеки Стратегія інформаційної безпеки України визначає, зокрема, збільшення кількості глобальних дезінформаційних кампаній; інформаційна політика рф як загроза не лише для України, але й для інших демократичних держав; деструктивний вплив соціальних мереж в інформаційному просторі; недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій; інформаційні маніпуляції щодо європейської та євроатлантичної інтеграції України тощо. Зазначається, що деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підриву стійкості суспільства та інформаційної дестабілізації держави. Серед стратегічних цілей та напрямів реалізації Стратегії визначені, зокрема, протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини... Окремо зазначається, що питання, пов'язані із кібербезпекою, визначаються Стратегією кібербезпеки України (від 26 серпня 2021 року № 447).

В Стратегії кібербезпеки України важлива роль приділяється кіберзагрозам саме в інформаційній сфері. Зазначається, що питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами. Рф залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій

стосовно національної інформаційної інфраструктури.

В Стратегії воєнної безпеки України передбачено, що всеохоплююча оборона України – це комплекс заходів, основний зміст яких полягає у: превентивних діях та стійкому опорі агресору на суші, на морі та в повітряному просторі України, протидії в ***кіберпросторі*** та нав'язуванні своєї волі ***в інформаційному просторі***. Відзначається, що на національному рівні рф залишається воєнним противником України, який здійснює збройну агресію проти України … системно застосовує воєнні, політичні, економічні, ***інформаційно-психологічні***, космічні, ***кібер-*** та інші засоби, що загрожують незалежності, державному суверенітету і територіальній цілісності України.

В пункті 3 Стратегії забезпечення державної безпеки визначено, що об'єктами забезпечення державної безпеки є державний суверенітет, конституційний лад, територіальна цілісність України, оборонний, економічний і науково-технічний потенціал, ***кібербезпека***, ***інформаційна безпека***, об'єкти критичної інфраструктури, державна таємниця та службова інформація. Відзначається, що рф для реалізації власних стратегічних цілей в Україні, у тому числі компрометації її державності, продовжує гібридну війну, системно застосовує політичні, економічні, інформаційно-психологічні та інші засоби, кібератаки.

В пункті 15 Стратегії зовнішньополітичної діяльності України наголошується, що ця Стратегія буде реалізовуватися, зокрема, на принципі стійкості, тобто здатності держави і суспільства ефективно протидіяти загрозам будь-якого походження і характеру, зокрема збройній агресії, економічному тиску, політичній дестабілізації, ***кібератакам***, ***дезінформації*** та іншим загрозам, адаптуватися до змін безпекового середовища, підтримувати стале функціонування, швидко відновлювати рівновагу після криз. В Стратегії енергетичної безпеки наголошується на високих ризиках кіберзагрози/кіберінцидентів щодо об'єктів критичної інфраструктури енергетичного сектору.

Отже, прийняті у 2020-2021 рр. безпекові Стратегії України є логічно взаємопов'язаними документами, реалізація яких ґрунтується на застосуванні механізмів забезпечення інформаційної безпеки і кібербезпеки України.

Література

1. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України: дис. … д-ра юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Запоріжжя, 2018. 518 с.