СУЧАСНІ КІБЕРЗАГРОЗИ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ТА ЗАХОДИ ПРОТИДІЇ

Мельник Д.С.,
канд. юрид. наук, провідний науковий співробітник
Міжвідомчий науково-дослідний центр з проблем
боротьби з організованою злочинністю при РНБО України

Процеси глобалізації та стрімкий розвиток технологій зумовили виникнення нових загроз національній критичній інфраструктурі, насамперед кібернетичних.

Так, окрім традиційних способів вчинення терористичних актів на об'єктах критичної інфраструктури, активно використовуються сучасні інформаційно-комунікаційні технології, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами. Дедалі більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти.

Все частіше об'єктами кібератак та проявів кібертероризму, кількість та потужність яких постійно зростає, стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій, наукових та медичних центрів.

Зазначені загрози набувають принципово нового значення в сучасних умовах ведення гібридної війни проти нашої держави та мають тенденції до посилення їх негативного впливу на стан національної безпеки в різних її сферах. Зокрема, наша держава стала полігоном для хакерських експериментів спецслужб іноземних держав, численних терактів і диверсій проти об'єктів критичної інфраструктури та їх співробітників. Упроваджувані хакерами шкідливі вірусні програми спершу апробувалися в Україні, а потім використовувалися у країнах Заходу.

Упродовж 2014-2020 років Україна зазнала безпрецедентної кількісті кібератак на інформаційні ресурси об'єктів критичної інфраструктури – підприємств життєзабезпечення, енергетичної, транспортної сфери, державних фінансових установ, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій тощо. Безпосереднього шкідливого впливу зазнали інформаційні системи та мережі на таких об'єктах.

Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її із ладу сталася ще у грудні 2015 року, коли російським хакерам із використанням троянської програми «BlackEnergy» вдалося атакувати комп'ютерні системи управління низки енергопостачальних компаній. Найбільше від кібератак

постраждали споживачі «Прикарпаття-обленерго», оскільки було вимкнено близько 30 підстанцій, біля 230 тисяч мешканців залишались без світла протягом 1 - 4 годин [1].

Наступна подібна кібератака сталась вночі з 16 на 17 грудня 2016 року. На понад одну годину була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берега м. Києва та прилеглих районів області [2]. Також у грудні 2016 року жертвами кібернападів з використанням модифікації вірусу «BlackEnergy» стали НБУ та низка державних банків разом з Мінфіном, Держказначейством та Пенсійним фондом України.

Протягом травня – липня 2017 року комп'ютерні системи КМ України, «Укренерго», «Київенерго», операторів зв'язку «Укртелеком», «Київстар», «Vodafone», «Lifecel», «Укрзалізниці», аеропорта «Бориспіль», низки державних фінустанов та багатьох комерційних структур в Україні зазнали масованої атаки вірусу «WannaCry» та мережевого черв'яка «Petya». У жовтні 2017 року комп'ютерні мережі «Київського метрополітену» та аеропорту «Одеса», а також інформаційні ресурси ДФС України та сайт держзакупівель «ProZorro» були атаковані з використанням вірусів «Locky» та «BadRabbit» [3].

Вже у січні 2018 року хакери зламали сервер Головного територіального управління юстиції в Одеській області, а у квітні - сайт Міненерговуглепрому України «www.mev.gov.ua».

У листопаді 2021 року правоохоронці викрили хакерське угруповування «Armagedon», учасники якого з 2014 року здійснили понад 5 тисяч кібератак на інформаційні ресурси державних органів України. Вони використовували власні вірусні програми і намагався «заразити» понад 1,5 тисячі урядових комп'ютерних систем. Основними цілями зловмисників були: контроль над об'єктами критичної інфраструктури (електростанції, системи тепло- та водопостачання); викрадення та збір розвідувальних даних, у т.ч. інформації з обмеженим доступом; проведення акцій інформаційно-психологічного впливу; блокування інформаційних систем [4].

Окрім того, електронні платіжні системи та криптовалюти активно використовуються для забезпечення функціонування каналів фінансування терористичної і сепаратистської діяльності в Україні та поза її межами [5].

Віддаленість доступу та анонімність таких кібератак сприяє їх активному проведенню противником проти нашої держави. В останні роки число кібератак дещо знизилося, однак кіберфахівцями спостерігається періодичне зростання їх кількості напередодні ключових подій у сучасних україно-російських «стосунках», що може свідчити про намагання сусідньої держави у такий спосіб «натиснути» на керівництво України та стимулювати до прийняття потрібних РФ рішень.

Таким чином, необхідність захисту об'єктів критичної інфраструктурив сучасних умовах зумовлює низка серйозних загроз національній безпеці, перелік яких визначений у Стратегії національної безпеки України, затвердженій Указом Президента України від 14.09.2020 № 392/2020, та доповнюється положеннями Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021. Серед них: сучасна модель глобалізації, яка уможливила поширення міжнародного тероризму, релігійного та ідеологічного фундаменталізму й екстремізму; продовження РФ гібридної війни проти України шляхом системного

застосування політичних, економічних, інформаційно-психологічних, кібернетичних і воєнних засобів; продовження спецслужбами іноземних держав, насамперед РФ, розвідувально-підривної діяльності проти України; комп'ютерний тероризм та комп'ютерна злочинність; посилення загроз для критичної інфраструктури, пов'язаних з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, триваючими бойовими діями, тимчасовою окупацією частини території України; використання ресурсів об'єктів критичної інфраструктури для фінансування тероризму, сепаратизму та розповсюдження зброї масового знищення тощо.

В умовах збройної агресії сусідньої держави та ведення нею гібридної війни проти України наявна в державі ситуація вимагає перегляду засад діяльності всієї системи забезпечення національної безпеки України, спрямованої на захист її критичної інфраструктури.

Зокрема, в таких умовах перед уповноваженими правоохоронними органами України постають нові завдання: протидія вищевказаним терористичним та іншим загрозам національній критичній інфраструктурі; організація належного захисту цієї інфраструктури шляхом забезпечення стійкості функціонування її систем і елементів, запобігання вчиненню терактів і диверсій, виникненню надзвичайних ситуацій на її об'єктах, припинення інших актів незаконного втручання в діяльність систем життєзабезпечення; упередження, стримування і недопущення настання тяжких наслідків тощо.

Разом з тим, на переконання фахівців, подальшу діяльність за цим напрямом необхідно зосереджувати не лише на постійному протистоянні противнику, але й створювати відповідні умови та адміністративні режими, за яких його підривні дії будуть неефективними.

Важливою передумовою такого підходу до організації дієвої системи забезпечення національної безпеки та захисту національних інтересів, яка зможе забезпечити ефективне функціонування системи захисту критичної інфраструктури, є запровадження в державі та постійне удосконалення відповідного контррозвідувального режиму, передбаченого Концепцією забезпечення контррозвідувального режиму в Україні, затвердженої Указом Президента України від 06.10.2017 № 310/2017.

Також потребує неухильного виконання Концепція створення державної системи захисту критичної інфраструктури України, схвалена КМ України 06.12.2017 № 1009 р., спрямованої на створення в державі системи управління безпекою критичної інфраструктури, визначення ролі і місця кожного державного органу у системі виявлення і нейтралізації загроз об'єктам, що мають стратегічне значення для безпеки держави.

Окрім цього, необхідно впровадити нещодавно прийнятий Закон України «Про критичну інфраструктуру» і національну Стратегію захисту критичної інфраструктури України, реалізація яких дозволить створити в державі ефективну систему захисту такої інфраструктури, координації та управління силами і засобами забезпечення її безпеки.

З урахуванням актуальних загроз і сучасних методів ведення гібридної війни проти України актуальним є посилення відповідальності за вчинення кібератак, диверсій та інших суміжних з ними протиправних дій на шкоду національній критичній інфраструктурі. З цією метою необхідно опрацювати питання щодо необхідності внесення відповідних змін до КК України із залученням компетентних фахівців уповноважених державних органів.

Реалізація викладених заходів у комплексі сприятиме забезпеченню надійного захисту об'єктів критичної інфраструктури в умовах ведення сусідньою державою гібридної війни проти України.

Список використаних джерел:

1. Міненерговугілля оприлюднило звіт про російську кібератаку на обленерго. URL: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat.

2. В Укренерго пояснили масштабний збій в енергосистемі під Києвом кібератаками URL: http://economics.unian.ua/energetics/1689781-v-ukrenergo-poyasnili-masshtabniyzbiy-v- energosistemi-pid-kievom-kiber-atakami.html.

3. Ще один фронт. Як Україна відповідає на виклики, що постали у віртуальному просторі. URL: http://tyzhden.ua/publication/183407.

4. В СБУ назвали перевод криптовалют основным механизмом финансирования ОРДЛО. URL: https://antikor.com.ua/articles/220214-vordlo.

5. В Україні викрили хакерів ФСБ, які здійснили понад 5 тисяч кібератак на держоргани. URL: https://ord-ua.com/2021/11/04/v-ukraini-vikrili-hakeriv-fsb-jaki-zdijsnili-ponad-5-tisjach-kiberatak-na-derzhorgani/.