УДК 343.851:004.056.53](477.54)

Русецький А. А.,
кандидат юридичних наук, депутат
Харківської обласної ради VII скликання

Марков В. В.,
кандидат юридичних наук, старший
науковий співробітник, декан факультету № 4
Харківського національного університету внутрішніх справ

АНАЛІЗ СТАНУ ЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ В ХАРКІВСЬКІЙ ОБЛАСТІ

ANALYSIS OF THREATS TO CRITICAL INFRASTRUCTURE IN KHARKIV REGION

Стаття присвячена питанням правового забезпечення захисту критичної інфраструктури в Харківській області, загрозам від проведення кібератак, які можуть бути націлені на інформаційно-телекомунікаційну критичну інфраструктуру та окремі її об'єкти. На основі аналізу чинного законодавства України та наукових досліджень за цією темою автором виділено найбільш вразливі об'єкти критичної інфраструктури Харківської області та наведено методичні рекомендації для вдосконалення рівня їх захисту від кібератак.

Ключові слова: *кібератака, критична інфраструктура, несанкціонований доступ, кібербезпека, Харківська область.*

Статья посвящена вопросам правового регулирования защиты критической инфраструктуры в Харьковской области, угрозам от проведения кибератак, которые могут быть направлены на информационно-телекоммуникационную критическую инфраструктуру и ее отдельные объекты. На базе анализа действующего законодательства Украины и научных исследований по данной теме автором выделены наиболее подверженные кибератакам объекты критической инфраструктуры Харьковской области и перечислены методические рекомендации для усовершенствования уровня их защиты от кибератак.

Ключевые слова: *кибератака, критическая инфраструктура, кибербезопасность, несанкционированный доступ, Харьковская область.*

The article deals with the legal coverage of critical infrastructure protection issues in Kharkiv region and the analysis of the threats of cyber attacks that can be targeted at information and telecommunication critical infrastructure and its separate objects. On the basis of the analysis of the current law of Ukraine and scientific studies in this field the author separates out the most vulnerable objects of Kharkiv region infrastructure and provides a list of methodological recommendations regarding their protection against cyber attacks.

Key words: *cyber attacks, critical infrastructure, unauthorized access, cyber security, Kharkiv region.*

Упродовж останніх років проблема належного захисту критичної інфраструктури постає все частіше. У зв'язку зі швидкісним розвитком суспільства та автоматизацією процесів управління і виробництва постала проблема інформаційного захисту від несанкціонованого втручання та доступу в автоматизовані системи критичної інфраструктури.

Значення терміну «критична інфраструктура» у національному законодавстві різних країн має деякі відмінності, але вони не є суттєвими. Зокрема, згідно з чинним законодавчим актом Сполучених Штатів, цей термін має таке тлумачення: «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище».

Відповідно до ч. 4 п. 2 Постанови Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» термін «критична інфраструктура» визначається як сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, довкілля, призвести до значних фінансових збитків та людських жертв [1].

Особливе місце в системі національної критичної інфраструктури України займає інформаційна інфраструктура, ефективний захист якої виступає необхідним елементом забезпечення її національної безпеки. Інформаційна інфраструктура охоплює безліч елементів критичної інфраструктури держави і, отже, може бути визначена як критична інформаційна інфраструктура.

До основних секторів критичної інфраструктури держави, що має тісний зв'язок з інформаційною інфраструктурою, належать системи управління в уряді, обороні, кредитно-фінансові і банківські системи, інформаційні системи науково-дослідного сектору, промисловості, енергетики (зокрема атомної), транспорту, водопостачання, комунального господарства, телекомунікації, цивільної оборони.

Перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави затверджується Кабінетом Міністрів України та належить до інформації з обмеженим доступом.

© А. А. Русецький, В. В. Марков, 2017

Визначається значне зростання інтенсивності проведення кібератак, які здійснюються на інформаційно-телекомунікаційну критичну інфраструктуру в Україні.

Відповідно до ч. 2 п. 2 Постанови Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», кібератакою є несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та націлені на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи [1].

Кібератаки націлені через глобальну мережу Інтернет на сервери державних установ, великих компаній, фінансових установ, політичних партій та ЗМІ, а останнім часом й на інформаційно-телекомунікаційну інфраструктуру воєнних об'єктів.

На окрему увагу заслуговує проблема забезпечення безпеки функціонування державних органів влади, Збройних сил, правоохоронних органів та спецслужб (будівель, належної інфраструктури тощо) у кризових ситуаціях. Відповідні інфраструктурні об'єкти у розвинутих країнах світу, як правило, також належать до критичної інфраструктури.

Аналізуючи наведені випадки здійснення кібератак, треба зазначити певні моменти. Характер і форми комп'ютерних нападів, від яких має бути розроблений захист, можуть істотно розрізнятися. Але, незважаючи на різноманітність типів атак, наслідки від них на найвищому рівні, як правило, включають:

– несанкціонований доступ або перехоплення інформації (втрата конфіденційності);

– несанкціонована зміна інформації, програмного забезпечення, обладнання і т. д. (втрата цілісності);

– блокування транзакцій та/або відключення системи (втрата готовності).

Загрози критичній інфраструктурі можна також розглядати не тільки з точки зору характеру їхнього походження, але й виділення елементів критичної інфраструктури, на які ці загрози націлені: фізичні елементи, зокрема, обладнання та ресурси об'єктів критичної інфраструктури; системи управління та комунікації, зокрема системи автоматичного управління та регулювання роботи об'єктів, системи зв'язку тощо; персонал об'єктів, зокрема диспетчерський, оперативний персонал, який безпосередньо забезпечує функціонування критичної інфраструктури у реальному часі.

Найбільшу загрозу безпеці об'єктів критичної інфраструктури становлять саме скоординовані атаки з використанням програмних вірусів. Такий вид атаки поєднує підготовчий етап (дії, що створюють на об'єкті нові уразливі місця) та атакуючі дії (використання уразливих місць). Водночас, підготовчі дії можуть здійснюватися значно раніше, ніж сама атака, можуть бути задіяні працівники (інсайдери) підприємства, що є об'єктом нападу, та здійснені різноманітні відволікаючі маневри.

Виділення спрямованості дії загроз методологічно дає змогу більш системно підійти до формування державної політики й організації системи захисту критичної інфраструктури [2].

Указом Президента України від 26 травня 2015 р. № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України»» затверджено Стратегію кібербезпеки України. Відповідно до положень п. 4.3 розділу 4 вищезазначеної Стратегії, кіберзахист критичної інфраструктури, перш за все, полягає в комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури [3].

Однією з вагомих причин загрози вчинення кібератаки на критичну інформаційну інфраструктуру України є відсутність єдиних регламентованих стандартів до кіберзахисту таких об'єктів. Саме тому вважаю за необхідне створити спеціальні підрозділи з кіберзахисту при об'єктах критичної інформаційної інфраструктури.

З огляду на це, потрібно встановити єдині кваліфікаційні вимоги для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз із упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам.

Отже, аналіз стану забезпечення інформаційної безпеки показує необхідність удосконалення системи адміністративно-правового регулювання інформаційної безпеки. Водночас постає потреба у виробленні нових засобів, методів і способів забезпечення інформаційної безпеки державного управління, моніторинг інформаційного середовища, наявності загроз та небезпек.

Удосконалення забезпечення інформаційної безпеки потребує цілеспрямованого вивчення зарубіжного досвіду організації і проведення інформаційних операцій, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів. Проведений нами аналіз надає можливість стверджувати, що система забезпечення інформаційної безпеки має бути міжвідомчою та ієрархічно організованою. її структура і організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів. Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління з конкретними відомчо-розпорядницькими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору.

Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багатобічної і багатоаспектної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування, тобто підтримувати стан гомеостазису.

Якщо розглядати критичну інфраструктуру на прикладі Харківської області джерелами загроз та викликів безпеці в інформаційній сфері можуть бути між-

народні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як «транзитного майданчику» для приховування атаки на інформаційні ресурси третьої сторони, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового, а в перспективі, не виключено, і воєнного характеру.

Враховуючи, той факт, що Харківська область територіально є найбільш наближеною до кордонів іншої держави та кордонів проведення Антитерористичної операції, а також наявність на території області досить потужних оборонних підприємств, держаних військових та невійськових установ та організацій, вона приваблює хакерів для ведення інформаційної війни, здійснення кібератак для нанесення шкоди важливим об'єктам життєзабезпечення населення області та держави в цілому.

Через таке геополітичне розташування Харківська область є об'єктом інтересів інших держав, організацій, транснаціональних корпорацій тощо, а отже, об'єктом їх інформаційно-психологічного впливу. З одного боку, розмаїття присутності вітчизняних та іноземних ЗМІ в інформаційному просторі сприяє диверсифікації джерел інформації, розвитку внутрішнього ринку інформації і, відповідно, утвердженню принципів свободи слова в нашій державі. З іншого боку, таке проникнення робить цю територію вразливою до зовнішніх інформаційно-психологічних впливів. Варто зауважити, що інтенсивність такого впливу не залежить значною мірою від політичних сил, що перебувають при владі в Україні, а зумовлена, насамперед, прагненням керівництва іноземних держав та міжнародних структур впливати на зовнішню та внутрішню політику нашої держави, а також має під собою політичне та економічне підґрунтя, продиктоване прагматичними підходами до забезпечення власних національних інтересів [5].

Також одним із найбільш уразливих об'єктів критичної інфраструктури є транспорт та транспортне сполучення. Втручання в національні, регіональні й муніципальні автоматизовані інформаційні та інформаційно-керуючи системи на транспорті – часто згадувана загроза для кібератак зловмисників. Але ми ще не перебуваємо на тому рівні, коли бізнес-процеси на транспорті залежать винятково від комп'ютерних мереж. Комунікації, які використовуються в інформаційно-комунікаційних системах транспорту, можуть і не залежати від інтернету. Високий ступінь залучення людини до транспортної логістики та керування процесами транспортування зменшують ризик кібератак. Але статистика інцидентів з інформаційною безпекою на транспорті поповнюється щороку [4].

Таким чином, для України взагалі та Харківської області окремо актуальні загрози та виклики в інформаційній сфері можна розмежувати за трьома напрямами:

– забезпечення технологічного розвитку – посилення внутрішнього цифрового розриву;

– захист інформації – вразливість до кібератак (зокрема на органи державної влади), незаконне поширення персональних даних, а також поширення інформації з порушенням авторських прав;

– інформаційно-психологічна безпека – широке застосування інформаційно-психологічних впливів зовнішніми та внутрішньодержавними суб'єктами інформаційних відносин на масову свідомість громадян.

ЛІТЕРАТУРА:

1. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23.08.2016 р. № 563 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF

2. Про рішення Ради національної безпеки і оборони України від 06.05. 2015 р. «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/287/2015.

3. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. / Зелена книга з питань захисту критичної інфраструктури в Україні [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf.

4. Стратегія кібербезпеки України : Указ Президента України № 96/2016 [станом на 15.03.2016 р.]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/96/2016.

5. Лахно В.А. Підвищення кібербезпеки транспорту в умовах деструктивного впливу на інформаційно-комунікаційні системи / В.А. Лахно, А.В. Грабарєв // Восточно-Европейский журнал передовых технологий. – 2016. – № 1(3). – С. 4–11 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/Vejpte_2016_1(3)__2.

6. Конах В.К. Зовнішні інформаційно-психологічні впливи на Україну та можливі шляхи їх нейтралізації / В.К. Конах, П.Д. Рогов // Сучасна українська політика. – 2013. – Вип. 29. – С. 135.

7. Про що мовчали новини у грудні 2013 р. // MediaSapiens. – 2014. – 1 серпня [Електронний ресурс]. – Режим доступу : http://osvita.mediasapiens.ua/material/26525.

8. Вознюк П.Ф. Інформаційно-психологічна боротьба і політична безпека держави: управлінський аспект / П.Ф. Вознюк / Наукові праці МАУП. – 2012. – Вип. 1(32), с. 59–69 / [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Npmaup/2012_1/pdf_files/59-69.pdf

9. Євсєєв В.О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду/ В.О. Євсєєв / Збірник наукових праць Харківського національного університету Повітряних сил. – 2016. – № 4(49). – С. 168–172 [Електронний ресурс]. – Режим доступу : http://www.hups.mil.gov.ua/periodic-app/article/17271.