вразливі групи «тюремного контингенту». Перед усім, слід амністувати людей старшого віку, інвалідів, тяжко хворих ув'язнених, які входять до групи ризику під час пандемії.

Література

1. Костантінова Надія. COVID-19 за гратами: правозахисники піддають сумніву офіційні дані. URL: https://www.radiosvoboda.org/a/covid-sizo-vyaznycia-testuvannia/30982701.html.

2. Романов М.В. Забезпечення прав і безпеки засуджених. *Вісник Асоціації кримінального права України.* 2021. № 1 (15). С. 256-275.

3. COVID-19, Prisons and Drug Policy. URL: https://www.hri.global/covid-19-prison-diversion-measures.

4. Проект Закону «Про внесення змін до деяких законодавчих актів України щодо запобігання виникненню і поширенню гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, в установах виконання покарань та місцях попереднього ув'язнення». URL: https://w1.c1. rada.gov.ua/ pls/zweb2/webproc4_1?pf3511=6865

5. Проект Закону «Про амністію засуджених (щодо запобігання поширенню гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2)». URL: https://www.kmu.gov.ua/bills/proekt-zakonu-pro-amnistiyu-zasudzhenikh-shchodo-zapobigannya-poshirennyu-gostroi-respiratornoi-khvorobi-covid-19-sprichinenoi-koronavirusom-sars-cov-2

6. Інформація Уповноваженого Верховної Ради України з прав людини, який виконує функції національного превентивного механізму, щодо імплементації в Україні Конвенції ООН проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання (подається в рамках розгляду сьомого періодичного звіту України щодо імплементації Конвенції на 70-й сесії Комітету проти катувань). С. 8-10. URL: https:// tbinternet.ohchr.org/Treaties/CAT/Shared%20Documents/UKR/INT_ CAT_ INP_ UKR_42469_O.PDF

УДК 343.98:004.56(043.2)

Гуцалюк М.В., к.ю.н., с.н.с., доцент,
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України, м. Київ, Україна
Клименко О.А., к.ю.н.,
Національний авіаційний університет, м. Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ЯК НЕОБХІДНА УМОВА РОЗВИТКУ ЦИФРОВИХ ТРАНСФОРМАЦІЙ СУЧАСНОГО СУСПІЛЬСТВА

Після пандемії Covid-19 у сучасному суспільстві значно прискорились цифрові трансформації у всіх сферах життєдіяльності. Водночас до нових

умов швидко адаптувалися кіберзлочинці, які використовують все нові схеми протиправної діяльності в глобальній мережі [1].

Європейська агенція кібербезпеки ENISA підготувала свій щорічний звіт Threat Landscape про стан загроз кібербезпеки, який визначає основні види загроз, основні тенденції, що спостерігаються щодо загроз, техніки нападу, а також описує відповідні заходи пом'якшення наслідків від кіберзагроз у 2021 році.

Протягом звітного періоду основні загрози, які були виявлені, включають: програми-вимагачі; шкідливе програмне забезпечення; cryptojacking; загрози, пов'язані з електронною поштою; загрози даним; загрози доступності та цілісності; дезінформацію; незловмисні загрози; атаки ланцюга постачання.

Програми-вимагачі були оцінені як основна загроза у 2020–2021 роках [2]. Збитки від кіберзлочинності у 2021 порівняно з 2016 роком за оцінками експертів збільшилися вдвічі й становлять 6 трильйонів доларів США.

Найбільш небезпечною є діяльність міжнародних хакерських угруповань, які здійснюють кібератаки на об'єкти критичної інфраструктури. Так, Державний департамент США оголосив винагороду в розмірі 10 мільйонів доларів за інформацію, що допоможе ідентифікувати осіб (або їхнє місцезнаходження), які займають керівні посади у транснаціональній організованій злочинній групі DarkSide. Раніше повідомлялося, що DarkSide проникла в мережу Colonial Pipeline і отримала майже 100 ГБ комп'ютерних даних. Захопивши дані, хакери вимагали викупу та загрожували витоком даних.

Як свідчать матеріали розслідувань за подібними кібератаками стоять не просто злочинні угруповання, а добре організовані професійні хакери, діяльність яких підтримується державними структурами [3].

У листопаді 2021 року в Польщі затримали громадянина України, якого підозрювали у кіберзлочинах за звинуваченням у зламі американської компанії Kaseya, що спеціалізується на розробці програмного забезпечення для керування мережевою інфраструктурою. Внаслідок кібератаки було паралізовано роботу принаймні 200 компаній у США, 800 шведських супермаркетів, 11 шкіл Нової Зеландії і двох IT-компаній Данії. Ймовірно, за атакою стояло хакерське угруповання з REvil, кіберзлочинці якого вимагали 70 мільйонів доларів викупу в криптовалюті для повернення вкраденої ними інформації. Підозрюваному українцю загрожує до 115 років ув'язнення, повідомляється на сайті Департаменту юстиції США, а його спільника, громадянина Росії, якого ще не вдалося затримати, очікують до 145 років позбавлення волі [4].

Для успішної боротьби з організованими хакерськими угрупованнями необхідне тісне міжнародне співробітництво правоохоронних органів [5].

У 2021 році Департаментом кіберполіції Національної поліції України

проведено дев’ять міжнародних операцій спільно з правоохоронцями США, Нідерландів, Франції, Німеччини, Великобританії, Норвегії, Ізраїлю, Кореї, Швейцарії, за підтримки Європолу та Євроюсту. У рамках міжнародної співпраці кіберполіцейські спільно з іноземними колегами провели понад 50 обшуків. Кіберзлочинці переважно спеціалізувалися на розробці вірусів, підтримці інфраструктури їх поширення, створенні фітингових сервісів. Фігуранти завдали збитків сотням європейських та американських організацій. Загальна сума збитків від протиправних дій хакерів становить 3,5 мільярди доларів США [6].

Водночас сучасні загрози у кіберпросторі потребують нових підходів щодо їх нейтралізації. Важливим етапом забезпечення кібербезпеки та протидії кіберзлочинності стало прийняття у серпні 2021 року нової Стратегії кібербезпеки України, у якій зазначено чіткі стратегічні цілі та методи їх досягнення [7].

Одним із головних напрямів на сьогодні залишається врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав – членів ЄС та враховуючи сучасні виклики й тенденції у сфері кібербезпеки і завершення імплементації в законодавство України положень Конвенції про кіберзлочинність.

Література

1. Клименко О.А., Гуцалюк М.В. Кримінальний опортунізм кіберзлочинності як загроза національній безпеці України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 1(58). С. 177–184. DOI: https://doi.org/10.18372/2307-9061.58.15326

2. ENISA Threat Landscape 2021. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

3. США готові заплатити $10 мільйонів за інформацію про хакерів, пов’язаних з РФ. URL: https://www.pravda.com.ua/news/2021/11/5/7312891/

4. Ukrainian Arrested and Charged with Ransomware Attack on Kaseya. URL: https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

5. Гуцалюк М.В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. *Інформація і право.* 2021. № 4(39). С. 141–147.

6. У 2021 році кіберполіція провела 9 міжнародних операцій із викриття хакерських угруповань. URL: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-provela--mizhnarodnyx-operaczij-iz-vykryttya-xakerskyx-ugrupovan-402/

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013