ГО «ГРУЗИНСЬКО-УКРАЇНСЬКИЙ ЕКСПЕРТНИЙ ЦЕНТР»

СУЧАСНІ ЗАГРОЗИ ГЛОБАЛЬНІЙ ТА РЕГІОНАЛЬНІЙ БЕЗПЕЦІ

МАТЕРІАЛИ
Міжнародної науково-практичної інтернет-конференції
(м. Одеса, 29 жовтня 2023 року)

DOI: 10.46340/GUEC2023-10

Одеса
Фенікс
2023

УДК 327.7:355.02
С 89

Сучасні загрози глобальній та регіональній безпеці : матер. С 89 Міжнар. наук.-практ. інтерн.-конф. (м. Одеса, 29 жовтня 2023 р.) [Електронне видання] / уклад. А. Полухіна ; ГО «ГУЕЦ». – Одеса : Фенікс, 2023. – 389 с. –Укр., англ., груз. мовами.

ISBN 978-617-8395-01-8

Збірник матеріалів містить матеріали доповідей, поданих на Міжнародну науково-практичну інтернет-конференцію «Сучасні загрози глобальній та регіональній безпеці», що відбулася 29 жовтня 2023 року. Подані матеріали були розглянуті під час роботи дев'яти секцій: теоретичні та прикладні аспекти міжнародного співробітництва у сфері безпеки; криза сучасної системи міжнародної безпеки; регіональна безпека в нових геополітичних концепціях; основні стратегічні напрямки кібербезпеки; кіберзахист і національна безпека: український досвід; цифрова дипломатія в умовах трансформації системи міжнародної безпеки; фейки та діпфейки як інструменти негативного впливу на національну безпеку; фактчекінг як інструмент протидії в гібридній війні; державне управління та національна безпека.

Збірник адресовано науковим, науково-педагогічним працівникам, здобувачам закладів вищої освіти, громадським організаціям, журналістам, незалежним експертам і всім, хто цікавиться проблемами загроз глобальній та регіональній безпеці.

УДК 327.7:355.02

ISBN 978-617-8395-01-8

ОСНОВНІ СТРАТЕГІЧНІ НАПРЯМКИ КІБЕРБЕЗПЕКИ

Сімакова Світлана Іванівна
кандидат юридичних наук, доцент,
Білоцерківський національний аграрний університет
соціально-гуманітарний факультет, м. Біла Церква, Україна

АКТУАЛЬНІ ПИТАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНСЬКОМУ СУСПІЛЬСТВІ

В сучасному суспільстві, яке є досить автоматизованим виникають нові види злочинів, які пов'язані із вчиненням шахрайства, крадіжок, вимагань із використанням транспортних телеконікаційних мереж. Захист інформаційних даних, та програмного забезпечення, які розміщені в мережі Інтернет від втручання злочинців (ворога) є важливим питанням в контексті забезпечення кібербезпеки в українському суспільстві. Розвиток кібербезпеки, кіберзахист – приорітетні напрямки нашої держави.

За статистичними даними, у 2022 р. комунікація між бізнесом та клієнтом у 72 % випавдках вілбулась у цифровому форматі. В такому разі споживачі очікують більш високий конроль над своїми даними та прозорості політики організацій. Про те, існує ризик втручання у особисті дані споживачів.

Наразі в українському суспільстві існує новий вид злочинця-кіберзлочинець. Це не просто злочинець, який вчиняє крадіжки, шахрайства, та інші види злочинів. Це злочинець, який володіє необхідними навичками роботи із транспортними телекомунікаційними мережами, програмним забезпеченням, різного роду обладнанням, тобто це особа, яка навчалась цьому, чи отримала такі знання працюючи на роботах пов'язаних із використанням транспортних телекомунікаційних мереж, Інтернетом.

Кіберзлочинці мотивовані жагою до легкої наживи, до збагачення за рахунок інших в найкоротші строки. Такі злочинці використовують банківські рахунки жерт злочину, намагаються отримати ідентифікаційні дані, дані банківських

карток. Дану інформацію злочинці можуть продати іншим особам, які зацікавлені в отриманні такої інформації, можуть викрасти кошти із банківських карток власника, можуть здіснювати прослідковування за життям власниками такого майна із корисних цілей, чи вчинити інші злочини. Такі злочини можуть стосуватись, як конкретної людини, так, і цілої сім'ї, чи навіть бізнесу. Захист бізнесу є приорітетним завданням власників бізнесу, адже для них є надважливим їхні клієнти та відповідно їх репутація, а коли компнія не може захистити клієнта то і довіри до неї не буде. А клієнт буде обирати вже інших партнерів для ведення бізнесу.

Захист підключених до мережі Інтернет, системобладнання, та програмного забезпечення та даних від кіберзагроз, кіберзлочинців називають кібербезпекою. Такий захист є вкрай необхідним, адже кіберзлочинці можуть підривати економічну безпеку, як громадян, так і суспільства загалом вчиняючи злочини в даній галузі. Cybersecurity" це безпека у звичайному нашому житті – це коли ми закриваємо двері свого помешкання, обладнуємо його засобами охорони, використовуємо сигналізацію для захисту свого автомобілю, та інше, а також це є наш захист тільки в IT просторі.

За статистичними даними Tech Times, кібератаки зловмисного програмного забезпечення на мобільні пристрої у всьому світі зросли на 500% протягом перших кількох місяців 2022 р. Наразі існують передові методи зламу захисту даних споживачів, такі, як: програми-вимагачі, фішинг атаки, атаки Man-in-the-Middle, та шкідливі програми та вебсайти.

У 2023 р. зафіксовано новий вид шахрайства з використанням deepfake, який полягає у створенні реалістічних аудіо та відео матеріалів створених за допомогою штучного інтелекту і машинного навчання. А тому правоохоронним органам під час розроблення заходів боротьби із кіберзлочинцями варто враховувати новітні види кібератак, задля попередження та розкриття кіберзлочинів.

З початку війни повномасштабної війни РФ проти України Міністерство цифрової трансформації створило першу в нашій державі українську IT армію. Метою якої є захист даних

у національному,та цифровому просторі. Під час повномаштабної війни проти України у 2020 р. було зафіксовано 800 повномаштабних кібератак. У 2021 р. 1400, У 2022 – понад 4000.

Кіберборотьба й кіберзахист стали одними із ключових елементів гібридної війни. Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають значних ударів у відповідь. У 2023 р. зафіксовано понад 1,25 мільйона DDoS-атак на російську інфраструктуру (це 8,4% від усіх кібератак у світі). За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО Наталії Ткачук, Україна – єдина держава, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії РФ (Кириченко).

У Стратегії кібербезпеки України визначено, що «забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі» (Задубінний; Указ про Стратегію кібербезпеки України).

Стратегія кібербезпеки України визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави (Задубінний; Указ про Стратегію кібербезпеки України).

Слушно вказує Андрій Задубінний: “РФ залишається одним з основних джерел загроз національній та міжнародній кібербезпеці. Надана оцінка діям країни-агресора, адже «Російська Федерація 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 гібридній війні проти України». Прогнозується зростання інтенсивності міждержавного протиборства й розвідувально-підривної діяльності у кіберпросторі.

Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій та посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед Російської Федерації, міжнародних хакерських угруповань для реалізації кібервпливу. У Стратегії також наголошується, що використання кіберпростору терористичними організаціями набуває глобального масштабу" ((Задубінний; Указ про Стратегію кібербезпеки України).

Висновок. Кібербезпека в українському суспільстві забезпечує поглиблення євроінтеграційних процесів шляхом уніфікації сучасних, дієвих методів забезпечення кібербезпеки із врахуванням практики ЄС і НАТО. В цьому нашій державі допомагають іноземні партнери, які розробляють спільні заходи спрямовані на посилення кіберстійкості України. Захист національних інтересів у кіберпросторі – приорітетні напрямки українського уряду. Єдина, могутня, нездоланна українська спільнота покладає всі зусилля на убезпечення кіберпростору для захисту суверенітету держави та розвитку суспільства; покликана захищати права, свободи і законні інтереси громадян України у кіберпросторі.

Література

Кириченко, А. *Кібербезпека в Україні: шляхи розвитку та можливості*. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html.

Задубінний, А. (2021). *Стратегія кібербезпеки України: цілі та пріоритети*. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/.

Указ про Стратегію кібербезпеки України 2021 (Президент України). *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/go/447/2021