МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

2. Бабійчук В. С. Кібертероризм та протидія йому. *Молодий вчений*. 2019. № 4 (68). С. 103–107. DOI: https://doi.org/10.32839/2304-5809/2019-4-68-24.
3. Калаянова О. Д. Кібертероризм – загроза інформаційній безпеці держави / Наукові проблеми запровадження правового режиму воєнного стану в Україні: сучасний вимір : Матеріали науково-практичного онлайн-заходу (м. Одеса, 29 квітня 2022 р.): ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ, 2022. С. 106–107.
4. Гриник Р. О., Пилипиенко В. М. Кібертероризм як нова форма міжнародного тероризму // Актуальні задачі та досягнення у галузі кібербезпеки : Матер. Всеукр. наук.-практ. конф. (м. Кропивницький, 23–25 листопада 2016 р.) URL: https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf (дата звернення: 30.09.2023).
5. Конрі-Мюррей Е. Політика безпеки в часи терору. URL: http://www.osp.ru/lan/2002/02/083.htm (дата звернення: 30.09.2023).
6. З початку повномасштабної війни СБУ заблокувала 76 ботоферм з аудиторією 3 млн фейкових акаунтів / Служба безпеки України ; Пресцентр. 2023. 6 листопада. URL: https://ssu.gov.ua/novyny/z-pochatku-povnomasshtabnoi-viiny-sbu-zablokuvala-76-botoferm-z-audytoriieiu-3-mln-feikovykh-akauntiv-illia-vitiuk (дата звернення: 07.11.2023).

БОРОТЬБА З КІБЕРЗАГРОЗАМИ У ПРОВІДНИХ ДЕРЖАВАХ АЗІЇ

Пядишев Володимир Георгійович
доктор юридичних наук, професор
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Прогрес у сфері кібернетичних систем та супутні проблеми, такі як кіберзлочинності не оминають і країни Азії. Отже у документі «Сфера загроз кібербезпеці Азії: 2022–2023», зокрема вказується, що Азіатсько-Тихоокеанський регіон був найбільш атакуваним регіоном у 2022 році. На нього припав 31% атак у всьому світі [1, с. 1]. Найчастіше жертвами кібератак ставали державні установи (22% від загальної кількості атак на організації), промислові компанії (9%), ІТ-компанії (8%) та фінансові установи (7%).

Головною загрозою для організацій і держав в Азії стає кібершпигунство. Отже 49% успішних атак на організації призвели до зламу конфіденційної інформації. Зловмисники полюють за даними користувачів і комерційними секретами. Уряди та організації вкладають значні кошти в дослідження та технології, що пояснює зростання активності банд кібершпигунства. Викрадення такого роду інформації може дати конкурентам технологічну перевагу.

Сінгапур. У Сінгапурі 2022 році спостерігалося 8500 випадків фішингу; понад 80% підробки у банках або у фінансовій службі [2, с.3]. Отже кількість спроб фішингу в цілі у Сінгапурі зросла на 175% до 8500, причому найбільше підробок у 2022 році було в банківському секторі [3, с. 1]. Відмічалося, що, нажаль, «закони про кібербезпеку все ще містять резерви для вдосконалення». Крім того, помітний брак міжнародної співпраці та єдиних регіональних стандартів.

Рекомендації до спільноти АСЕАН щодо підвищення кіберстійкості організацій включають визначення неприпустимих подій і захист критичних активів, моніторинг і реагування на кіберзагрози за допомогою передових інструментів безпеки, оцінку ефективності впроваджених заходів і навчання співробітників.

Південна Корея. Світ потребує політики кіберзахисту та стійкості даних, які пропонують різноманітні гнучкі, доступні та прості у використанні рішення. У Кореї може бути кращий спосіб, ніж універсальні підходи, які пробували деякі інші країни [4, с. 4]. У висновках документу «Співпраця Південної Кореї та НАТО у сфері кібербезпеки» [5, с.2] вказується, що Південна Корея та НАТО виводять свої відносини на новий рівень відповідно до Індивідуальної програми партнерства, погодженої в липні 2023 р. З усіх сфер, у яких вони поглиблюють зв'язки, кібербезпека виділяється як пріоритет для обох. Сеул і

Трансатлантичний альянс мають можливості та спільні інтереси для розвитку широкого партнерства в цій сфері.

У передмові до документу «Національна стратегія кібербезпеки» Управління національної безпеки Республіки Корея у квітні 2019 Президент Південної Кореї пан Мун Чже Ін відмічав, що : Республіка Корея є лідером у світі в галузі інформаційно-комунікаційних технологій (ІКТ) і відповідної інфраструктури, а розвиток різноманітного та зручного кіберпростору дозволив людям розширити свій кругозір. Однак нещодавнє зростання кіберзлочинності та тероризму загрожує життю звичайних людей і комерційній діяльності компаній. Систематичні та складні кібератаки становлять серйозну загрозу національній безпеці. Уряд держави розробив Національну стратегію кібербезпеки. В основі кібербезпеки лежать люди, і уряд розробив **три основні принципи** кібербезпеки, щоб захистити людей.

- Ми гарантуватимемо основні права громадян і здійснюватимемо безпекову діяльність, засновану на верховенстві права.
- Ми реалізуємо чітку та прозору кібербезпеку, забезпечуючи участь громадян.
- Ми можемо захистити наш кіберпростір тільки завдяки співпраці уряду, компаній та громадян.

Отже, уряд Південної Кореї докладе всіх зусиль для створення відкритого та безпечного онлайн-середовища [6, с. 3].

Японія. У грудні 2022 р. в Японії фірмами Nikkei Inc. і Nikkei Business Publications, Inc. Було організовано подію «Кіберініціатива Токіо 2022». Тут зібралися провідні експерти з кібербезпеки, які працюють у промисловості, уряді та наукових колах з Японії та за кордоном, щоб обговорити останні тенденції. в галузі кібербезпецки, а також підходи до протидії загрозам кібератак [7, с. 1]. Зокрема відмічалося, що «вторгнення росії в Україну вплинуло на те, як усі думають про кіберпростір. Отже, все більше і більше людей розуміють життєво важливе значення кібербезпеки. Вказувалося, що ключовим фактором, що лежить в основі стрімкого зростання кількості кібератак проти японських компаній, є зростання використання Інтернету завдяки просуванню цифрової трансформації.

В останні роки все більше японських компаній позиціонують безпеку як частину своєї стратегії управління безпекою з точки зору безперервності бізнесу. Було вказано, що «діапазон знань, необхідних для ключових посад безпеки, розширився». Важливо запровадити комплексне управління кризовими ситуаціями на основі чіткого розуміння ризиків, пов’язаних з ІТ.

У документі «Ландшафт загроз Японії» від вересня цього року вказується, що технологічний прогрес Японії йде у паралель з підвищеною увагою як спонсорованих державою, так і недержавних суб’єктів кіберзагроз, що, зокрема, обумовлено ескалацією економічної та технологічної конкуренції з боку таких країн, як Китай і Південна Корея [8, с. 1].

При чому у сенсі так званих «контрнаступальних кібероперацій» між державами, Японія має свої проблему на конституційному рівні. Отже, незалежні «контрнаступальні кібероперації» залишаються обмеженими статтями 9 і 21 післявоєнної конституції Японії. Стаття 9 забороняє Японії проводити превентивні кібератаки, тоді як стаття 21 обмежує збір розвідкою даних з відкритих джерел і перешкоджає розвідувальному співтовариству Японії здійснювати кіберрозвідку. Іншими словами, зобов’язання уряду «заздалегідь усунути можливість серйозних кібератак» вимагає поглибленого нового тлумачення або навіть перегляду Конституції 1947 року. Тому довгострокова державна підтримка урядової політики має першорядне значення для того, щоб успішний «активний кіберзахист» пустив коріння в мисленні японців [9, с. 5].

16 грудня 2022 року уряд Японії схвалив рішення кабінету міністрів щодо стратегічних документів, пов’язаних із безпекою: Стратегії національної безпеки (СРБ – NSS), Стратегії національної оборони (СНО – NDS) і Програми розбудови оборони (ПРО – DBP) [10, с. 2].

Відображаючи нову NSS, у бюджеті на 2023 фінансовий рік Міністерство закордонних справ планує використовувати штучний інтелект для посилення моніторингу інформаційного простору та посилення аналізу розвідувальних даних. Міністерство оборони також планує запровадити автоматичну систему збору та аналізу інформації за допомогою технології штучного інтелекту для розуміння ситуації інформаційної війни.

Що стосується питання активного кіберзахисту, пропозиція Ліберально-демократичної партії, яка описує стратегію кібервідповіді як «необхідну для розгляду впровадження активного кіберзахисту від зловмисника», була просто перенесена у Стратегію національної безпеки таким чином: «Японія запровадить активний кіберзахист для завчасного усунення можливості серйозних кібератак». Для реалізації активного кіберзахисту Національний центр готовності до інцидентів та стратегії кібербезпеки буде реструктуризовано, щоб створити нову організацію з кібербезпеки, яка координуватиме політику у сфері кібербезпеки та керуватиме кіберпідрозділами Сил оборони та поліції Японії. .

Чисельність кіберперсоналу в поточній «Середньостроковій програмі оборони на 2019 – 2023 фінансові роки» становить близько тисячі, але у відповідь на вказівку в Програми розбудови оборони, Міністерство оборони навчить 4000 «кібервоїнів» і забезпечить кібернавчання 16 000 співробітників JSDF протягом п’яти років.

Крім того, кілька законів будуть переглянуті для впровадження активного кіберзахисту.

Малайзія. За останнє десятиліття малайзійський шлях цифрової трансформації досяг значних успіхів, оскільки всі сектори та підприємства в усьому світі намагаються оцифрувати свої основні процеси, щоб працювати краще в динамічному бізнес-середовищі. Однак у міру переходу держави до цифрового простору, кібербезпека стає серйозною проблемою. На думку головного виконавчого директора з кібербезпеки Малайзії, Д-ра А. А. Вахаба кіберзлочинці більше не прив’язані до однієї особи. Вони борються з компаніями і гігантами та кидають виклик безпеці нації в цілому. Отже надзвичайно важливо повністю розуміти ці загрози та ризики, використовуючи відповідні засоби захисту та продуктивні функції [11, с. 3]. Малайзійські організації стикаються з трьома грізними кіберзагрозами: 1) зловмисним програмним забезпеченням, 2) атаками програм-вимагачів, 3) зломом паролів. Ці загрози, визначені 64% організацій, вважаються головними проблемами в системі кібербезпеки країни. Перехід до хмарних сервісів і додатків породив новий набір проблем, оскільки цифрові транзакції стрімко зросли та наражали бізнес на підвищені кіберризики (55%). Крім того, зростаюча залежність від хмарних служб і програм (53%) і поширення незахищених пристроїв Інтернету речей (IoT) (49%) додають складності, що вимагає ретельного розгляду.

Висновки

Проблеми з кіберзагрозами не оминають і держави Азії. Тут найвищій рівень кіберзлочинності у світі та рік від року він зростає. Головною загрозою в регіоні стає кібершпигунство.

Тут вважається, що вторгнення росії в Україну вплинуло на розуміння життєво важливого значення кібербезпеки.

Серед перешкод у боротьбі з кіберзлочинністю тут вважаються відставання вдосконалення законодавства, брак міжнародної співпраці та брак єдиних регіональних стандартів.

Серед шляхів підвищення ефективності з кіберзагрозами тут вважається впровадження штучного інтелекту для посилення моніторингу інформаційного простору та посилення аналізу розвідувальних даних, вдосконалення державних структур по боротьбі з кіберзагрозами, поєднання зусиль держав та промисловості, а також виведення відносин з НАТО на новий рівень.

Література:

1. Cybersecurity threatscape of Asia: 2022–2023. *PTSecurity.com. Published on September 12, 2023*. Site. URL: https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/ (дата звернення: 01.11.2023).

2. Chia O. 8,500 phishing cases in Singapore in 2022; more than 80% spoofed a bank or financial service. The StraiTstimes. June 27, 2023. Site. URL: https://www.straitstimes.com/tech/phishing-attempts-doubled-in-2022-as-scams-ransomware-attacks-continue-to-plague-s-pore-csa (дата звернення: 01.11.2023).
3. Tham D. Phishing attempts on Singapore targets rose 175% to 8,500, with banking sector most spoofed in 2022. *Channel News Asia. 23 Jun 2023*. Site. URL: https://www.channelnewsasia.com/singapore/cybersecurity-csa-phishing-ransomware-ai-3578216 (дата звернення: 01.11.2023).
4. Kim S. J., Bae S. Korean Policies of Cybersecurity and Data Resilience. *Carnegie Endowment for International Peace. August 17, 2021*. Site. URL: https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164 (дата звернення: 01.11.2023).
5. South Korea-NATO cybersecurity cooperation: learning to work together in the face of common threats. *Real Instituto Elcano.* 04 Oct 2023. Site. URL: https://www.realinstitutoelcano.org/en/analyses/south-korea-nato-cybersecurity-cooperation-learning-to-work-together-in-the-face-of-common-threats/ (дата звернення: 01.11.2023).
6. National Cybersecurity Strategy. *Republic of Korea National Security Office. April 2019.* Site. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf (дата звернення: 01.11.2023).
7. Cyber Initiative Tokyo 2022. *NIKKEI Asia*. 2022. Site. URL: https://ps.nikkei.com/cit2022/ (дата звернення: 01.11.2023).
8. Japan Threat Landscape. *Cyfirma.Com*. *2023-09-23*. Site. URL: https://www.cyfirma.com/outofband/japan-threat-landscape/ (дата звернення: 01.11.2023).
9. Brans A. Japan’s evolving cybersecurity landscape: a latecomer at a crossroads. *Asia Power Watch. 21 July 2023*. Sote. URL: https://asiapowerwatch.com/japans-evolving-cybersecurity-landscape-a-late-comer-at-a-crossroads/ (дата звернення: 01.11.2023).
10. Osawa J. How Japan Is Modernizing Its Cybersecurity Policy. *Stimson.Org. February 2, 2023*. Site. URL: https://www.stimson.org/2023/japan-cybersecurity-policy/ (дата звернення: 01.11.2023).
11. Abdullah I.N. Malaysia's Cybersecurity Wake-Up Call. *CybersecurityASEAN. Sep 14, 2023*. Site. URL: https://cybersecurityasean.com/daily-news/malaysias-cybersecurity-wake-call (дата звернення: 01.11.2023).

КІБЕРЗЛОЧИННІСТЬ, ЯК СУЧАСНЕ ЯВИЩЕ; МОЖЛИВІ ШЛЯХИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Д’яков Андрій Володимирович
кандидат технічних наук, доцент кафедри інформаційного
та аналітичного забезпечення діяльності
правоохоронних органів факультету №2 ІПФПНП ЛьвДУВ
Зачек Олег Іванович
кандидат технічних наук, доцент, заступник завідувача кафедри
інформаційного та аналітичного забезпечення діяльності
правоохоронних органів факультету №2 ІПФПНП ЛьвДУВ
Магеровська Тетяна Валеріївна
кандидат фізико-математичних наук, доцент, доцент кафедри інформаційного
та аналітичного забезпечення діяльності правоохоронних
органів факультету №2 ІПФПНП ЛьвДУВ

Кіберзлочинність є однією з найактуальніших проблем сучасного світу і представляє собою злочинну діяльність, пов'язану з використанням інформаційних технологій та комп'ютерних систем. Це явище є сучасним, оскільки воно почало набирати обертів і ставати серйозною загрозою для суспільства внаслідок розвитку і поширення інтернету, комп'ютерів, мобільних пристроїв та інших технологічних засобів.

ЗМІСТ