НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

РІЧНИЙ АНАЛІТИЧНИЙ ОГЛЯД

Жовтень 2023 - вересень 2024

Ця публікація стала можливою завдяки підтримці, наданій Агентством США з міжнародного розвитку, згідно з умовами гранту Української фундації безпекових студій в рамках Проєкту USAID "Кібербезпека критично важливої інфраструктури України".
Думки автора, висловлені в цій публікації, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США.

ЗМІСТ

АКРОНІМИ

CERT-UA	**Урядова команда реагування на комп'ютерні надзвичайні події України**
CISA	**Cybersecurity and Infrastructure Security Agency**
CYBERCOM	**United States Cyber Command**
DDoS	**distributed denial-of-service attack**
ENISA	**European Union Agency for Cybersecurity**
FBI	**Federal Bureau of Investigation**
JICA	**Japan International Cooperation Agency**
NIS2	**NIS 2 Directive (Directive (EU) 2022/2555)**
NIST	**National Institute of Standards and Technology**
NSA	**National Security Agency**
USAID	**United States Agency for International Development**
ГУР МО	**Головне управління розвідки Міністерства оборони України**
ДССЗЗІ	**Державна служба спеціального зв'язку та захисту інформації України**
ЄС	**Європейський Союз**
ІТ	**Інформаційні технології**
Мінцифра	**Міністерство цифрової трансформації України**
НАТО	**Організація північноатлантичного договору**
НКЦК	**Національний координаційний центр кібербезпеки при РНБО України**
ОКІ	**об'єкти критичної інфраструктури**
ОТ	**операційні технології**
ПЗ	**програмне забезпечення**
СБУ	**Служба безпеки України**

ВСТУП

За 5 місяців до початку повномасштабного вторгнення Україна ухвалила нову Стратегію кібербезпеки України – документ, що визначав пріоритети кібербезпекового розвитку на наступні 5 років.

24 лютого 2022 року Україна зіткнулася з екзистенційним викликом для свого існування – масштабна військова агресія з боку росії здійснювалася всіма можливими засобами, включаючи кібератаки. Ця постійна кіберзагроза залишається важливим фактором впливу на національну систему кібербезпеки, і є визначальним елементом для діяльності українських кібербезпекових стейкхолдерів.

Однак протягом останніх років стає помітною ще ціла низка тенденцій чи процесів, що можуть мати істотний вплив на кібербезпекову ситуацію як у світі, так і в Україні: зростання протистояння в кіберпросторі між державами, вплив ШІ та квантових технологій на сферу кібербезпеки, зростання загроз ОТ інфраструктурі, кіберзагрози для космічних об'єктів та посилення ролі підводної цифрової інфраструктури – лише декілька з таких тенденцій.

Україна входить в період оцінки стану реалізації чинної Стратегії кібербезпеки та підготовки її нової редакції. Це вимагає врахування не лише поточної кібербезпекової ситуації, але і ширшого розуміння ландшафту кіберзагроз, тенденцій у сфері кібербезпеки, політики ключових українських партнерів (в частині тих заходів, які вони вживають для поліпшення власної кібербезпеки), а також оцінку того, що вже зроблено Україною для підвищення своєї кіберстійкості.

Цей Звіт охоплює період з четвертого кварталу 2023 року по третій квартал 2024 року включно і має на меті запропонувати огляд ключових тенденцій та подій за цей період, вказавши на ті елементи, які Україна може врахувати при створенні нового документа довгострокового планування у сфері кібербезпеки.

I. ГЛОБАЛЬНІ ТРЕНДИ

ЗАГОСТРЕННЯ КОНКУРЕНЦІЇ МІЖ США ТА КИТАЄМ У КІБЕРПРОСТОРІ

Відносини між США та КНР у сфері кібербезпеки все більше набувають рис жорсткого суперництва, характерного для першої декади 2000-х років. У лютому 2024 року слухання перед Спеціальним комітетом Палати представників з питань Комуністичної партії Китаю висвітлили зростаюче занепокоєння безпекових органів США щодо китайської кіберактивності. Все жорсткіші оцінки отримують дії китайських хакерських груп. Органи безпеки США (NSA, CISA, Міністерство оборони США) попереджають, що у разі кінетичної атаки на Тайвань, можливою є одночасна атака на ОКІ США, особливо об'єкти військової критичної інфраструктури. Крім того, кібердіяльність Китаю тепер також поширюється на операції впливу з використанням штучного інтелекту та дезінформації.

Серед угрупувань, які отримали багато уваги цього року – група Volt Typhoon, метою якої є дестабілізація та створення паніки у суспільстві, особливо під час потенційних конфліктів. Вперше угруповання Volt Typhoon ідентифікувала компанія Microsoft в травні 2023 року. В березні 2024 кібербезпекові органи США разом з союзниками, такими як Австралія, Нова Зеландія, Канада та Великобританія у лютому випустили спільні настанови щодо діяльності угрупування. В них йдеться, що Китай не лише збирає інформацію та займається шпигунською діяльністю, а проникає до мереж США та їх союзників з метою порушити функціонування критичної інфраструктури, щоб створити хаос. Угруповання застосовує метод атаки "Living-Off-the-Land," і його діяльність набагато складніше виявити, особливо якщо атакована організація використовує традиційні інструменти безпеки, які шукають відомі скрипти або файли зловмисного ПЗ. Діяльність Volt Typhoon є одним з індикаторів переходу китайських проурядових хакерських груп від традиційного шпигунства до більш загрозливих дій, аж до кібердиверсій.

Також, увагу до себе привертали низка інших китайських угрупувань. APT41 стала предметом пильної уваги кібербезпекових компаній в липні 2024 року. Компанія Zscaler опублікувала технічний звіт про особливості діяльності цього угрупування, кібербезпекова компанія Mandiant попередила про спроби APT41 проникнути в глобальний транспортний і технічний сектори, а кіберексперти Cisco Talos виявила зловмисну кампанію APT41, що скомпрометувала тайванський урядовий науково-дослідний інститут. Інше угруповання, Flax Typhoon, вдалося знешкодити американським правоохоронцям, які конфіскували скомпрометовані пристрої, контрольовані цією групою. Згідно з даними FBI, група заразила «сотні тисяч» пристроїв по всьому світу в рамках операції з компрометації і викрадання даних. У вересні стало відомо, що китайська хакерська група Salt Typhoon зламала кілька інтернет-провайдерів у США, а на китайських кранах, які працюють в американських портах, виявили приховані бекдори, встановлені без відома користувачів.

Разом з тим, в США стикнулись з ширшим розумінням своєї вразливості через відкритість своїх мереж до китайської загрози. Дослідження компанії Fortress

Information Security продемонструвало, що майже все програмне забезпечення, використовуване енергетичними компаніями США, містить код від російських і китайських розробників та з великою ймовірністю має критичні вразливості, які можуть знаходитися в режимі очікування понад 4 роки. У травні національна розвідка США опублікувала звіт, у якому зазначається, що Китай залишається найбільшою кіберзагрозою для Сполучених Штатів, зокрема в контексті виборів, де китайські хакери використовують штучний інтелект для розпалювання соціальної напруги. У вересні були прийняті рішення та розпочаті обговорення, які можуть суттєво вплинути на кібербезпеку в країні. Зокрема, це стосується обмеження використання кранів китайського виробництва у портах, а також китайських та російських технологій в автомобілях.

Масштаб загрози підкреслює кількість китайських пристроїв в мережах США. На початку квітня 2024 року видання Axios навело оцінки дослідників, які свідчать про те, що станом на лютий 2024 у комерційних мережах США працювало близько 300 000 пристроїв від 473 китайських виробників, або 3,8% усіх американських пристроїв, підключених до Інтернету. Відносно лютого 2023 року ця цифра зросла на 85 000 пристроїв.

Китай, своєю чергою, звинувачує західні країни у дезінформаційних кампаніях щодо себе, стверджуючи, що історія навколо діяльності кіберугрупування Vault Typhoon – це результат спланованої операції NSA, FBI та інших американських відомств за участі розвідувальних служб країн «П'яти очей». Також, наприкінці квітня Альянс індустрії кібербезпеки Китаю (CCIA) випустив звіт «Загрози США та саботаж безпеки та розвитку глобального кіберпростору», в якому стверджується, що для збереження своєї глобальної гегемонії, Сполучені Штати «зловживають своєю перевагою» у сфері інформаційних технологій і ресурсів, займаючись прослуховуванням і шпигунством, спотворюючи громадську думку, маніпулюючи суспільними настроями, підриваючи правила та роз'єднуючи ланцюги постачання.

КИТАЙ АКТИВІЗУЄ КІБЕРШПИГУНСЬКУ ДІЯЛЬНІСТЬ ЩОДО ЄС

Загострення все частіше вибудовується не лише по лінії США-КНР, але і Європа-КНР. Особливо помітно це стало у березні 2024 року навколо цілої низки звинувачень на адресу китайських хакерських груп щодо втручання в роботу парламентських структур по всьому світу:

- Міністерство юстиції США оприлюднило висновок про те, що китайські хакери атакували європейських законодавців, зокрема членів Міжпарламентського альянсу з питань Китаю;
- британський уряд офіційно звинуватив Китай у кібератаках на демократичні інститути Великобританії;
- Фінляндія приписує злам фінського парламенту китайському угрупованню APT31;
- новозеландський уряд звинуватив КНР у кібератаках проти парламенту країни у 2021 році.

У другій половині року китайські хакери здійснили атаку на Голову парламентського комітету закордонних справ Бельгії. Нідерланди також виявили масштабну шпигунську кампанію китайських хакерів, які провели складну операцію з проникнення у військові мережі країни. У червні військова розвідка Нідерландів повідомила, що розслідування інциденту триває, і масштаби втручання виявилися значно більшими, ніж спочатку передбачалося.

ДЕРЖАВИ ВСЕ ЧАСТІШЕ ПУБЛІЧНО ЗАЯВЛЯЮТЬ ПРО КІБЕРНАСТУПАЛЬНІ ОПЕРАЦІЇ ТА СТВОРЮЮТЬ КІБЕРСИЛИ

Кібервимір російсько-української війни змінює і багаторічне статус-кво щодо наступальних кібероперацій – традиційно держави про них не повідомляли й до останнього заперечували свою участь в них.

Українські державні органи, часто у співпраці з кіберволонтерами, ведуть наступальні операції проти рф у кіберпросторі. Хоча вперше про наступальні кібероперації українська влада публічно заявила у листопаді 2023 року, справжній сплеск припав на 2024 рік. У першому кварталі 2024 року військова розвідка України заявила про здійснення атаки проти одного з російських постачальників IT систем для промисловості та на російську систему управління дронами, що призвело до втрати росіянами доступу до серверів. ГУР МО також атакувало як приватні, так і державні структури рф, які фінансують російську агресію проти України. В липні українська військова розвідка разом із кіберволонтерами атакувала майже сотню російських веб вебресурсів.

Загалом, другий та третій квартали 2024 року були відмічені активно наступальною діяльністю з боку українських державних та недержавних кіберфахівців. Проукраїнське хакерське угруповання Blackjack успішно здійснило операцію проти інфраструктури російського «Москолектору». У червні російські енергетичні компанії, IT-компанії та державні установи стали жертвами трояна Decoy Dog, що спричинило збої в роботі супермаркетів по всій країні. Група Sticky Werewolf атакувала російську фармацевтичну компанію та науково-дослідний інститут, що займається мікробіологією та розробкою вакцин. Також було здійснено масштабну атаку на великі російські банки, що зробило їхні послуги недоступними для деяких користувачів.

Країни по всьому світу уважно спостерігають за цими змінами у динаміці кіберпротистояння і змінюють власну політику (або активізують наявну) щодо посилення своїх військових кіберпідрозділів. Так керівництво ЄС розпочало обговорення створення європейських кіберсил, що будуть мати наступальні можливості. Німеччина планує створити окремий рід військ – кіберсили, щоб швидше реагувати на нові загрози та посилити свою кібероборону. А Китай завершує масштабну реформу своїх кіберсил, створивши у квітні 2024 року Сили інформаційної підтримки.

ПРОЦЕС PALL MALL

В лютому 2024 року Великобританія та Франція спільно провели першу установчу конференцію, присвячену боротьбі із загрозою комерційного кіберрозповсюдження. Під цим терміном мається на увазі безконтрольне поширення створених комерційними фірмами інструментів, які можуть використовуватись з протиправною метою для наступальних кібероперацій. За результатами конференції учасники підписали декларацію Процесу Pall Mall, яка фіксує плани учасників ініціативи вивчати альтернативні політики та інноваційні методи боротьби з цією загрозою. Наразі Ізраїль майже не бере участі у цих ініціативах, адже ізраїльські компанії мають значну частку на експортному ринку шпигунського ПЗ.

ЗРОСТАННЯ УВАГИ ДО КІБЕРБЕЗПЕКИ КОСМІЧНИХ ОБ'ЄКТІВ

Супутники відіграють ключову роль у світовій комунікаційній, навігаційній та безпековій системі, що зумовлює підвищення уваги до їх безпеки в контексті глобального протистояння, що загострюється. В США поширюється розуміння, що супутники можуть стати мішенню для кібератак противника, що може призвести до переривання сигналу, перехоплення, або повного відключення супутника. З метою більш системного реагування на проблему, CISA вивчила чи є потреба в нових вимогах безпеки для космічних засобів, а також у розширенні можливості реагування на інциденти. Агенція випустила настанови для операторів космічних систем. Крім того, на випадок атаки, CISA має на меті посилити підтримку критичної інфраструктури, яка залежить від можливостей космічного базування. Законодавці в Сенаті США представили законодавство для посилення кібербезпеки супутників, вимагаючи від CISA розробити відповідні онлайн-ресурси, а від Білого дому – створити федеральну стратегію боротьби з кіберзагрозами для супутникових систем. Втім, її розгляд знаходиться лише не початковому етапі. NIST випустив настанови щодо кібербезпеки у космічній галузі.

БЕЗПЕКА ПІДВОДНИХ КАБЕЛІВ ТА КОНКУРЕНЦІЯ ЗА НИХ

Інциденти з фізичною безпекою підводних кабелів можуть мати довгострокові наслідки для глобальної доступності мережі Інтернет. У травні увагу до теми підводних кабелів привернув інцидент, під час якого чотири основні підводні кабелі передачі даних, що обслуговують Африку, були сильно пошкоджені в районі Кот-д'Івуару. Це сталося всього через кілька тижнів після того, як поблизу Ємену був розірваний інший кабель. Це вплинуло на доступ до Інтернету в Африці, а також на обмін даними між Африкою та Європою. Для запобігання таким наслідкам Європейська комісія видала Рекомендації щодо безпеки та стійкості підводної кабельної інфраструктури, в яких, серед іншого, йдеться про покращення координації всередині ЄС, як з точки зору управління, так і фінансування.

Передбачається, що підводні кабелі стануть наступним полем бою між Китаєм та США. У жовтні двопартійна група американських сенаторів закликала адміністрацію Байдена провести «перегляд існуючих вразливостей глобальної підводної кабельної інфраструктури, включаючи загрозу саботажу з боку росії, а також зростання ролі Китайської Народної Республіки в прокладанні та ремонті кабелю», а Федеральна комісія зі зв'язку заявила, що прийме рішення щодо перегляду глобальної мережі підводних комунікаційних кабелів, які обслуговують майже весь світовий Інтернет-трафік у контексті питання національної безпеки.

ОСОБЛИВА УВАГА ДЕРЖАВ ДО РОЛІ КВАНТОВИХ ТЕХНОЛОГІЙ

Світ активно готується до появи та розповсюдження квантових технологій. Так, в січні 2024 року, НАТО прийняло свою першу квантову стратегію, ЄС готується до впровадження постквантової криптографії для запобігання появі нових кіберзагроз. Єврокомісія вже випустила рекомендації для країн-членів, які вказують на необхідність розробки відповідних дорожніх карт для цього переходу.

Постквантове шифрування знову стало важливою темою в урядових та експертних дискусіях після оприлюднення NIST стандартів для трьох базових алгоритмів, стійких до квантових обчислень. Великобританія вже включила ці стандарти у свої стратегічні документи. Також дослідження RAND, опубліковане в серпні, вивчає можливості квантових обчислень і штучного інтелекту для зміцнення потенціалу Міністерства національної безпеки США.

IBM передбачувала, що у 2024 році стане більше кібератак з метою крадіжки зашифрованих даних в надії отримати доступ до їх вмісту із появою квантових комп'ютерів.

ВПЛИВ ШІ НА КІБЕРБЕЗПЕКУ

Станом на кінець 2023 року деякі провідні компанії, що надають послуги у сфері кібербезпеки, дійшли висновку, що вплив штучного інтелекту (зокрема, ChatGPT) на кібербезпекову ситуацію був перебільшеним, адже помітним був лише вплив у сфері фішингу. Разом з тим, увага до цієї теми не загасала протягом всього періоду.

Влітку фахівці з кібербезпеки Unit42 навчили ШІ створювати дієве зловмисне ПЗ, використовуючи релевантну базу вихідних даних. Створене ШІ ПЗ виявилось не лише ефективним, але й здатним оперативно модифікуватися, створювати численні варіації та адаптуватися до різних платформ. Фахівці з Horizon3.ai вже пропонують нові сервіси з підтримкою ШІ для пришвидшення визначення пріоритетів кіберзахисту та усунення вразливостей у кібербезпеці організацій.

У червні 2024 року CISA провела перші командно-штабні навчання, присвячені загрозам від ШІ, та офіційно висловила занепокоєння щодо можливого впливу ШІ на зростання кіберзагроз у хімічному та біологічному секторах. Одночасно з

цим, урядові структури США шукають способи застосування ШІ для підвищення безпеки. Міністерство оборони США наразі розглядає можливості використання ШІ для оперативного реагування на кібератаки.

В серпні CISA призначила керівника відділу ШІ, а NSA запустила платформу автоматизованого тестування на проникнення на основі ШІ. Експерти аналізують вплив ШІ на кібербезпекові операції. Серед загальних висновків, ШІ розглядається більше як вдосконалення існуючих інструментів, ніж їхня заміна.

Активним в цьому процесі є і ЄС. 12 липня 2024 року набрав чинності ключовий регуляторний документ ЄС у сфері штучного інтелекту (ШІ) – Акт про Штучний Інтелект (Artificial Intelligence Act). Документ ухвалила Європейська Рада 21 травня 2024 року, а сама розробка документа розпочалась ще у квітні 2021 року і пройшла декілька раундів дискусій та модифікацій. Хоча документ загалом стосувався питань розвитку самого ШІ, він охопив і кібербезпекову тематику. Це питання піднято в документі в контексті використання перевірених наборів даних, можливих атак на легітимний ШІ, метою яких є не виведення системи з ладу, а наповнення її «отруєними» наборами даних. Відповідно Акт вимагає, щоб розроблені алгоритми ШІ були кіберстійкими, належно захищеними, а ключовим органом з кібербезпеки ШІ стане ENISA.

II. КІБЕРІНЦИДЕНТИ, ЩО МАЛИ МІЖНАРОДНЕ ЗНАЧЕННЯ

КІБЕРАТАКИ ПРОТИ ЛОКАЛЬНИХ СИСТЕМ ВОДОПОСТАЧАННЯ

Кібератаки проти локальних систем водопостачання окремих невеликих громад в США стали новим трендом від початку моніторингового періоду. У середині січня CISA разом з партнерами опублікували «Керівництво з реагування на інциденти для сектору систем водопостачання та водовідведення», яке має допомогти організаціям побудувати свій кіберзахист. Проте, власники таких компаній кажуть, що у них часто взагалі відсутні ресурси на заходи кіберзахисту. Аналітики пропонують державі запроваджувати заходи підтримки та стимулювання, щоб допомогти компаніям забезпечити належний рівень кіберзахисту

Разом з тим, дослідження демонструють, що багато промислових організацій не дотримуються навіть найпростіших стандартів кібербезпеки. Через низку успішних кібератак за останні пів-року Агентство з охорони навколишнього середовища США (EPA) провело перевірки, які виявили, що понад 70% систем водопостачання не відповідають Закону про безпечну питну воду та мають критичні кібервразливості. Управління звітності уряду США (GAO) закликало Агентство з охорони довкілля провести термінову комплексну оцінку ризиків у всьому секторі та розробити стратегію з урахуванням ризиків.

У жовтні повідомлялося про зростання кількості хакерських атак проти водної інфраструктури США, причому деякі з них були пов'язані з геополітичними суперниками США, включаючи Іран, росію та Китай. Ці атаки показали, наскільки локальний рівень залишається незахищеним перед кіберзагрозами – там ще більш серйозно відчувається брак кадрів та фінансових ресурсів для належного кіберзахисту.

АТАКА НА CHANGE HEALTHCARE

Лютий та березень 2024 стали випробуванням і для американської системи охорони здоров'я. Наприкінці лютого відбулась атака хакерів Blackcat проти систем Change Healthcare (частина UnitedHealth Group), яка обробляє близько 50% запитів до медичних страхових компаній у США. До її мережі входять близько 900 000 лікарів, 33 000 аптек, 5 500 лікарень і 600 лабораторій. Ця атака призвела до негативних наслідків для всієї системи охорони здоров'я країни, яка сильно залежить від страхування.

За масштабами цей інцидент порівнюють із Colonial Pipeline, але у медичному секторі. Хакери вкрали значний обсяг персональних даних клієнтів компанії, в результаті чого генеральний директор свідчив перед Палатою представників США. Розслідування та слухання у Сенаті виявили, що компанія виплатила викуп у розмірі 22 мільйонів доларів. Були також виявлені численні недоліки у політиці кібербезпеки, включаючи слабкий захист персональних даних та невідповідність кадрової політики кібербезпековим настановам щодо наявності досвіду роботи в кібербезпеці для CISO організації. Загальні втрати організації перевищили 800 мільйонів доларів і, за попередніми оцінками, можуть досягти одного мільярда.

В червні жертвою подібної за масштабом атаки стала британська компанія Synnovis, яка займається клінічними дослідженнями, і є ключовим партнером Національної служби здоров'я (NHS) Великобританії. За припущеннями, російські хакери атакували цю медичну установу, вимагаючи викуп у розмірі 50 мільйонів доларів. Британські правоохоронні органи все ще розслідують цей інцидент, який, ймовірно, призведе до змін у кібербезпековій політиці Великобританії у сфері охорони здоров'я. Загалом, сектор охорони здоров'я залишається однією з найулюбленіших цілей хакерів, адже медичні заклади часто мають слабкі системи захисту та зберігають велику кількість персональних даних.

CROWDSTRIKE

Через недостатнє тестування чергового оновлення продукту 19 липня 2024 року виник supply chain інцидент, що вплинув на понад половину компаній зі списку Fortune 500. Проблеми виникли в лікарнях, були скасовані авіарейси по всьому світу – загалом інцидент стосувався 8,5 млн Windows-пристроїв (пристрої на Apple та Linux не постраждали). Реакція постраждалих компаній (Delta Air Lines) та країн (Малайзія) вже спрямована на відшкодування збитків від компаній CrowdStrike, або Microsoft, або від страхових установ, але перспектива цього залишається невизначеною. Ймовірним довгостроковим наслідком інциденту стане чіткіше формулювання розділів про відповідальність у контрактах з кібербезпековими хмарними організаціями та посилення регуляції хмарних сервісів з боку держав

ВРАЗЛИВІСТЬ НУЛЬОВОГО ДНЯ IVANTI CONNECT SECURE

Вразливість нульового дня Ivanti Connect Secure стала інструментом для кібершпигунської діяльності китайського угрупування UNC5221. Виявлена у січні 2024 року, вона залишалася актуальною протягом першого кварталу 2024 року. 6 лютого була опублікована Спільна заява про дві додаткові вразливості Ivanti Connect Secure і Ivanti Policy Secure. Європейська Комісія, ENISA, CERT-EU, Європол та мережа CSIRTs ЄС повідомили, що нові виявлені вразливості дозволяють зловмисникам виконувати команди в системі. NSA підтвердило, що зловмисники, використовуючи вразливість Ivanti Connect Secure, атакували підприємства оборонного сектору, а CISA була навіть змушена

відключити декілька своїх систем від мережі, аби не допустити кібератаки на них. 4 квітня Ivanti випустила виправлення для вразливостей DoS, які впливають на Ivanti Connect Secure та Ivanti Policy Secure. У всіх підтримуваних версіях Ivanti Connect Secure та Ivanti Policy Secure було виявлено та виправлено чотири вразливості.

III. АКЦЕНТИ У ПОТОЧНОМУ ЛАНДШАФТІ КІБЕРЗАГРОЗ

КІБЕРАТАКИ З ПОЛІТИЧНИМ ПІДҐРУНТЯМ

Все більшого розповсюдження набувають політично вмотивовані атаки. За результатами дослідження ENISA, опублікованого в грудні 2023 року, 60% DDoS атак наразі мають політичне підґрунтя. Згідно зі звітом NETSCOUT за 2024 рік, кількість DDoS на критичну інфраструктуру зросла на 55% за останні чотири роки, причому ескалацію спричиняють політично мотивовані кіберактори. Фахівці з кібербезпеки прямо кажуть, що групам реагування на кіберінциденти доведеться слідкувати не лише за своїми інформаційними системами, але і геополітичними подіями які стають каталізатором нових загроз для державного та приватного секторів.

ВРАЗЛИВОСТІ ОТ СЕРЕДОВИЩА

Атаки на промислові системи, включаючи не лише IT-інфраструктуру власників, але й операційні технології (OT), стають дедалі інтенсивнішими. Це викликає занепокоєння, адже захист OT-систем часто є значно слабшим у порівнянні з IT, а багато контролерів просто не мають доступних оновлень безпеки. Власники промислових об'єктів нерідко недостатньо обізнані про кіберзагрози. Зокрема, зараз майже 100 000 систем управління доступні через Інтернет, і вразливості для таких систем з'являються все частіше (особливо з урахуванням нових 0-day у промислових маршрутизаторах).

Протягом останнього кварталу кілька організацій опублікували важливі рекомендації щодо кібербезпеки для OT. CISA надала рекомендації для OT-систем з відкритим кодом, а NSA запровадила репозиторій OT Intrusion Detection Signature and Analytics. Приватний сектор також бере участь у підвищенні безпеки: компанія Dragos у рамках програми Community Defense Program пропонує інструменти малим організаціям для захисту їхньої OT-інфраструктури. Так, у лютому Siemens виявив 275 нових вразливостей у продуктах для автоматизації виробництва. Звіт Dragos Inc. підтверджує зростаючу увагу кіберзловмисників до цієї сфери, виявляючи, що за 2023 рік ще три кіберугруповання почали активно орієнтуватися на OT-інфраструктуру, збільшуючи загальну кількість відомих груп до 21.

Проблема захисту таких систем є дуже складною, оскільки підприємства часто знають про вразливості, але не можуть їх усунути через завершення гарантійного терміну старих систем або через технологічні і бізнесові обмеження. Власники об'єктів відзначають, що регуляторний процес для OT фрагментарний і суперечливий, що ускладнює забезпечення кібербезпеки відповідно до секторальних стандартів. Вони також вказують на труднощі та високу вартість модернізації OT-систем.

Станом на зараз, індустрія кібербезпеки і уряд активно працюють над захистом промислових об'єктів, які є пріоритетними для національної безпеки. Згідно зі звітом Censys, близько половини з 40 000 промислових систем управління (ICS) у США залишаються вразливими через слабкі протоколи безпеки, особливо в системах автоматизації будівель. На тлі кібератак на Halliburton та Microchip дослідники виявили недостатню координацію між IT та OT-командами у майже половині компаній.

Застарілі системи залишаються ще однією проблемою. За даними корпорації MITRE, деякі федеральні системи, яким понад 60 років, все ще експлуатуються, що загрожує безпеці у довгостроковій перспективі через відсутність кваліфікованих фахівців для їх обслуговування. SANS Institute також відносить експлуатацію застарілих систем до п'яти найвищих загроз для кібербезпеки у майбутньому.

Загалом, кіберспеціалісти продовжують наголошувати на критичних вразливостях промислових систем, але реальних кроків для їх усунення ще небагато. Наприклад, компанія Bitsight нещодавно виявила щонайменше сім критичних вразливостей у системах автоматичного вимірювання (ATG), що використовуються в великих резервуарах, які дозволяють отримати повний адміністративний доступ до цих пристроїв.

БОРОТЬБА З ПРОГРАМАМИ-ВИМАГАЧАМИ

Рансомвер залишається серед основних викликів, з якими стикаються бізнеси, критична інфраструктура, навчальні заклади, місцеве самоврядування та адміністрації у всьому світі. Середня сума початкового викупу від ransomware у 2023 році сягнула 600 тисяч доларів США, і зловмисники продовжують націлюватися на нові сектори, такі як сектор розваг та казино. Протягом аналізованого періоду відбулось декілька успішних операцій правоохоронних органів для зменшення загроз від таких угрупувань.

- в 4-му кварталі 2023 року американські правоохоронці припинили роботу угрупування Hive. Його лідерів було оголошено у розшук. Державний департамент США оголосив винагороду за інформацію про лідерів цих угруповань.
- важливою подією у лютому 2024 року стала вдала операція британських правоохоронців проти потужної ransomware групи Lockbit, на чию долю припадає значна частина ransomware атак по всьому світу. Зусилля британських правоохоронців були доповнені діями української поліції, яка заарештувала двох учасників цього угруповання.
- у другому кварталі 2024 року британська поліція зупинила діяльність LabHost, яка надавала злочинцям послуги Phishing-as-a-Service, що використовувалися для створення початкових точок вторгнення в мережі жертв.
- інша операція була проведена в травні 2024 року британськими, американськими та австралійськими правоохоронцями з метою розкриття особи лідера кіберзлочинної групи LockBit, яким виявився росіянин Дмитро Хорошев. Держдепартамент США оголосив винагороду у розмірі 10 мільйонів доларів за інформацію, яка дозволить його затримати.

Проте наразі важко сказати чи матимуть ці заходи довгостроковий ефект. Вже у травні 2024 року експерти Trellix виявили, що інфраструктура, яка належала угрупованню LockBit, активно відновлюється і знову починає функціонувати.

Протягом моніторингового періоду, на додачу до боротьби з інфраструктурою злочинців та конкретними групами, США розглядали посилення заходів із недопущення виплати викупів аж до повної заборони виплат викупів хакерам-здирникам. Вважається, що такі заходи зменшать мотивацію злочинців до зловмисних дій. Проте це питання викликає спротив з боку деяких стейкхолдерів. Вони занепокоєні тим, що такі обмеження можуть поставити під загрозу їхнє функціонування у випадку кібератаки. Зловмисники, зі свого боку, все частіше вдаються до нестандартних засобів тиску, включаючи фізичний тиск на потенційних жертв атак, як це відбулося у випадку з діяльністю групи UNC3944.

ВИТОКИ ДАНИХ

Витоки даних як з державних, так і з приватних систем, є постійним явищем. У вересні сталось одразу декілька помітних кіберінцидентів пов'язаних з витоками даних. Зокрема, були розкриті особисті дані всіх нідерландських поліцейських. Кібербезпекова компанія Proton виявила на DarkWeb персональні дані близько 3000 співробітників Конгресу США, а Microchip Technology підтвердила викрадення інформації під час атаки з використанням програм-вимагачів. У відповідь на подібні інциденти Федеральна комісія зв'язку США (FCC) змусила T-Mobile витратити 31,5 мільйона доларів на покращення кібербезпеки після систематичних витоків даних протягом трьох років. А, наприклад, індійська компанія Star Health подала до суду на Telegram за те, що платформа не протидіяла спробам поширення викрадених даних її клієнтів.

IV. СПОЛУЧЕНІ ШТАТИ АМЕРИКИ

ІМПЛЕМЕНТАЦІЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Відповідно до нової Стратегії кібербезпеки, США розширює коло партнерів по всьому світу, одночасно з цим шукаючи нові способи безпечно обмінюватись інформацією з найбільш довіреними партнерами. У 2024 році було укладено цілу низку міжнародних угод про партнерство: між ENISA та CISA, формування нового партнерства між США, Південною Кореєю та Японією. Одночасно військові органи США шукають більше практичних шляхів взаємодії з акцентом на Тихоокеанський регіон. CYBERCOM США розширює практику спільних кібернавчань з партнерами в цьому регіоні, НАТО залучає Японію та Південну Корею до своїх навчань в межах Cyber Coalition 2023, а Пентагон будує спеціальну мережу Mission Partner Environment для обміну інформації з Філіппінами та Тайванем. Ці зусилля додатково посилені кібердопомогою, яку США через свій військовий бюджет планує надати Тайваню в найближчі роки – це чітко вказує на основні занепокоєння військового командування США в частині недопущення ще однієї ескалації військової ситуації у світі.

Поява першого в американській практиці чіткого плану виконання Стратегії кібербезпеки США вказує на те, що Білий Дім хоче докласти більше зусиль до контролю за цим документом, більш чіткого розуміння хто і за що відповідає при його реалізації, а також створити прозорий механізм визначення результатів його імплементації. Очільник Офісу національного кібердиректора Гері Кокер, призначений наприкінці 2023 року, серед іншого зосереджений саме на цій контрольно-координаційній функції.

ВПРОВАДЖЕННЯ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ

У третьому кварталі США розширили обов'язкові вимоги кібербезпеки для науково-дослідних організацій, що фінансуються федеральним бюджетом. Останній меморандум Офісу національного кібердиректора (ONCD) зобов'язує державні агентства прискорити перехід до архітектури Zero Trust, надавши стратегію протягом 120 днів, і впровадити квантово-стійке шифрування.

ЗАПРОВАДЖЕННЯ ПІДХОДУ SECURE BY DESIGN

Підхід Secure by Design набуває все більшої ваги в державній політиці ключових країн. CISA активно просуває свою платформу Secure by Design Pledge – добровільну ініціативу, яка об'єднує компанії, що беруть на себе зобов'язання дотримуватися принципів Secure by Design. Великобританія також готується до впровадження цього підходу для учасників ринку.

КІБЕРБЕЗПЕКА ВИБОРІВ В США

Хоча самі вибори відбулись 5 листопада, вже після закінчення моніторингового періоду, підготовку до них вели, як американські посадовці, так і приватні гравці протягом більшої частини року. Агентство з кібербезпеки та захисту інфраструктури США (CISA) контролювало безпеку виборів на всіх етапах, надаючи консультації та розповсюджуючи рекомендації для забезпечення кібер- і фізичної безпеки. CISA також відпрацювала процедури захисту виборчого процесу на прикладі «супервівторка» у березні 2024 року. Компанія Мета інформувала, що як Китай, так рф будували мережі онлайн впливу напередодні виборів у США. Китай, Іран і росія чинили значний тиск на виборчий процес, поширюючи дезінформацію, фейкові новини та підбурюючи до радикалізму. За даними Microsoft, найбільш активним у втручанні був Китай. Іран і росія також продовжують свої традиційні дії, але цього разу іранські хакери були особливо активні, проводячи довготривалі операції з викрадення даних учасників виборів, атакуючи кампанію Дональда Трампа і намагаючись поширити викрадену інформацію. У відповідь на це Міністерство юстиції США висунуло звинувачення трьом іранцям.

У серпні увага була прикута до спроб зламу інформаційних систем обох президентських команд, причому команда Трампа звинуватила іранських хакерів. Компанії Microsoft, Google і Meta також повідомили про зростання іранської кіберактивності, пов'язаної з виборами. 19 серпня Офіс директора національної розвідки (ODNI), FBI та CISA зробили спільну заяву про посилення іранських спроб втручання у вибори США.

ВРАЗЛИВІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

За інформацією американського уряду, 80% кранів типу «судно-берег», що переміщують товари в портах США, виготовляються в Китаї. Розслідування Конгресу щодо вантажних кранів китайського виробництва виявило комунікаційне обладнання, яке, як видається, не є необхідним для підтримки їх нормального функціонування, і це може становити прихований ризик для національної безпеки.

НЕСТАЧА РОБОЧОЇ СИЛИ У КІБЕРСЕКТОРІ

Станом на червень 2024 року, за даними помічника національного кібердиректора США Сієу Мо, попри деякі позитивні зрушення в США все ще існувало близько 500 тисяч незаповнених вакансій кіберфахівців у всіх секторах економіки. Це логічно призводить до підвищення уваги уряду США до освітньої складової. Офіс національного кібердиректора США (ONCD) активно просуває імплементацію Національної стратегії кіберосвіти та робочої сили, прийнятої ще влітку 2023 року, проводячи дискусії з учасниками ринку. Все частіше лунають думки про відмову від вимоги вищої освіти при наймі кіберфахівців на

користь підтвердженої кваліфікації. Ще наприкінці 2023 року компанія Trend-micro зазначала, що організації нереалістично формують запити на фахівців з кібербезпеки, що ускладнює їх пошук і формує брак робочої сили. Зниження вимог має допомогти також Міністерству оборони, яке наразі має близько 27 тисяч незаповнених кібервакансій через бюрократичні проблеми.

V. ЄВРОПЕЙСЬКИЙ СОЮЗ

АДАПТАЦІЯ ЗАКОНОДАВСТВА ТА ОРГАНІЗАЦІЙНИХ СТРУКТУР ДО НОВИХ ВИКЛИКІВ

У квітні 2024 року Європарламент ухвалив Акт про кіберсолідарність. Поряд з тим, що документ має зміцнити загальні можливості ЄС щодо виявлення, ситуаційної обізнаності та реагування, але також сконцентрується на двох важливих аспектах:

- створення кіберрезерву на рівні ЄС (через інструменти залучення допомоги від надійних приватних постачальників)
- впровадження інструментів тестування безпеки ОКІ.

Ці дві новели багато в чому пов'язані із рефлексією ЄС щодо українського досвіду ведення кібервійни.

Також ЄС оприлюднив плани розробки Закону про космос, що включатиме питання кібербезпеки – це особливо актуально на фоні зростаючих зусиль державних та приватних компаній з освоєння космічного простору (в тому числі через виведення супутникових систем на орбіту).

В жовтні 2024 року Європейський Союз прийняв Акт про кіберстійкість (Cyber Resilience Act). Цей документ створює нові рамки функціонування для ІТ сектору та виробників ІТ обладнання, вимагаючи від них більше уваги до заходів кібербезпеки. Швидше за все імплементація цього документа буде складною та відбуватись з різною швидкістю в європейських країнах.

Більшість цих зміни є реакцією на зміни у ландшафті кіберзагроз з яким стикається ЄС – європейські компанії (особливо в енергетичному секторі) стикаються із все більш помітними інцидентами, що можуть зачепити сам процес надання їх основних послуг. Також, ці зміни кореспондуються із довгостроковими оцінками кіберзагроз, які регулярно оприлюднює ENISA. Звіт «Передбачення загроз кібербезпеці до 2030 року» від березня 2024 року якраз вказує на загрози ланцюжкам поставок, застарілу цифрову інфраструктуру, що може піддаватись додатковим кібер ризикам, загрози з боку нецільового використання ШІ.

Намагаючись створити більш гнучкі механізми реагування на інциденти, у травні 2024 року Європейська Рада схвалила Керівні настанови, що сприятимуть створенню гібридних груп швидкого реагування. Такі групи (які розгортаються за запитом) потрібні для підготовки та протидії гібридним загрозам і кампаніям впливу у сьогоднішньому світі. Вони будуть орієнтовані на протидію дезінформації, кібератакам, атакам на критичну інфраструктуру тощо. Гібридні групи мають стати одним із ключових інструментів для підтримки держав-членів ЄС і країн-партнерів у протидії гібридним загрозам у рамках EU Hybrid Toolbox.

СКЛАДНОСТІ ІЗ ЗАПРОВАДЖЕННЯМ ПРАВИЛ КІБЕРБЕЗПЕКИ

Зусилля, спрямовані на посилення кібербезпеки ОКІ, включаючи готовність Брюсселю інвестувати в кібербезпеку, слабко корелюється з реальною ситуацією в цій сфері. Звіт ENISA у листопаді 2023 року чітко вказує на те, що хоча кіберчастка IT-бюджету ОКІ досягла 7,1% у 2022 році, однак це лише на 0,4% більше ніж у 2021. Крім того, 47% ОКІ не планують наймати фахівців з кібербезпеки протягом наступних двох років, при цьому 83% організацій стверджують, що мають труднощі з наймом принаймні в одній сфері інформаційної безпеки. В попередні місяці ENISA публікувала схожі дослідження, які показують аналогічні тенденції – власники ОКІ або не бажають інвестувати в кібербезпеку, або не вважають це за потрібне. Враховуючи ці тенденції та загальний характер нормативних змін до яких вдається ЄС останнім часом, можна передбачити, що європейське законодавство у сфері кібербезпеки буде ставати все більш жорстким та ультимативним, а його порушення буде вести до значних штрафів для компаній (як це є у сфері застосування GDPR).

Брак готовності європейських стейкхолдерів витрачати кошти на кібербезпеку змушує ЄС вдаватись до двох стратегій: посилення регуляції та запровадження інструментів фінансової підтримки. Наприклад, у серпні 2024 року оприлюднено нову програму спрямовану на підвищення рівня кіберзахисту в ЄС. У рамках цієї ініціативи оголошено конкурс для європейських постачальників послуг кібербезпеки, які бажають долучитися до надання послуг країнам ЄС і їхнім об'єктам критичної інфраструктури відповідно до Директиви NIS2. Програма реалізується в межах Програми цифрової Європи (DEP), для її реалізації планується використати 28,3 млн євро.

СЕРТИФІКАЦІЯ ПРОДУКТІВ ІКТ

У 1 кварталі запрацювала перша європейська схема сертифікації для продуктів ІКТ відповідно до Загальних критеріїв. Схема містить елементи різних національних схем сертифікації і має на меті зробити використання ІТ продуктів європейськими споживачами більш безпечним. Наразі схема лише в процесі впровадження, але ЄС покладає значні надії на неї та подальший розвиток.

VI. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

КЛЮЧОВІ КІБЕРІНЦИДЕНТИ

Фахівці команди CERT-UA продовжують моніторити тенденції у сфері кібербезпеки. У другій половині 2024 року вони зафіксували підвищений інтерес з боку ворожих хакерів до українського телекомунікаційного сектору. Атаки на військових, спрямовані на отримання доступу, контролю та викрадення розвідувальної інформації зі спеціалізованих систем ситуаційної обізнаності залишаються стратегічною військовою ціллю противника. Серед груп, які здійснюють атаки на Україну, найактивнішими є ті, що наразі не асоційовані з офіційними спецслужбами країни-агресора, хоча вони діють в інтересах російської влади. Звіт Держспецзв'язку «російські кібероперації H1'2024» вказує на нову тенденцію: зловмисники активно використовують месенджери та інші комунікаційні засоби, видаючи себе за знайомих жертви. Вони надсилають шкідливі файли, маскуючи їх під документи або відео, що стосуються військової тематики.

У грудні 2023 року відбулась серйозна кібератака проти одного з національних операторів мобільного зв'язку – Київстар. Наслідки атаки – щонайменше декілька днів абоненти компанії не могли скористатись жодним зв'язком, а процес відновлення розтягнувся на декілька тижнів. Це доводить, що відсутність руйнівних кібератак протягом 2-х років війни є не лише результатом ефективних кіберзахисних дій, але і можливо все ще не виявленими позиціями ворожих хакерів в інформаційних системах. Для попередження нових масштабних атак українські кіберфахівці активно вивчили наслідки цієї кібератаки. За даними СБУ, російські хакери готували другу хвилю атак, яка мала нанести ще більше шкоди оператору.

У січні 2024 було здійснено декілька особливо потужних кібератак – одна з них була спрямована на банківський сектор, а інша помітно вплинула на один з найбільших дата-центрів України. Останнє призвело до порушення доступності послуг декількох державних організацій та інформаційних систем.

НАРОЩУВАННЯ СПРОМОЖНОСТЕЙ

Україна продовжує нарощувати власні спроможності щодо реагування на кіберінциденти. Зокрема, розширює практику проведення кібернавчань (наприклад, Національним координаційним центром кібербезпеки (НКЦК) проведено змагання з кібербезпеки HackWave та INCIDENT RESPONSE DAYS 2.0, а також відбулись перші секторальні кібернавчання для транспортного сектору CIREX.CoBridge), запускає нові інструменти кібергігієни (наприклад Мінцифра запустила тест на знання правил безпеки в мережі «Кіберграм», а ДССЗЗІ провела всеукраїнський онлайн-урок з кібербезпеки для понад 20

тисяч глядачів) та стимулює інновації в секторі кібербезпеки. Для посилення кіберстійкості регіонів в липні НКЦК організував перший Regional Cyber Resilience Forum у Львові, який зібрав близько 400 учасників.

Україна, за підтримки міжнародних партнерів, активно розвиває систему підготовки кадрів у сфері кібербезпеки, акцентуючи на практичних заходах. За ініціативи НКЦК у Національному авіаційному університеті було презентовано перший національний кіберполігон Cyber Range UA. Також у Київському політехнічному інституті ім. Ігоря Сікорського відкрито «Лабораторію кібербезпеки автоматизованих систем управління».

УЧАСТЬ УКРАЇНСЬКИХ ПРАВООХОРОНЦІВ У МІЖНАРОДНИХ ПОЛІЦЕЙСЬКИХ ОПЕРАЦІЯХ

Протягом моніторингового періоду українські правоохоронці регулярно долучалися до міжнародних операцій по боротьбі з кіберзлочинністю. У жовтні-листопаді 2023 року їм вдалось провести декілька успішних операцій проти міжнародних груп кіберзлочинців. Один з найбільших успіхів – ліквідація угрупування, яке за допомогою ransomware заподіяла шкоду на 80 мільйонів доларів. Ці успіхи доповнюються іншими операціями Кіберполіції спільно з чеськими колегами, а також операцією проти групи, яка починаючи з 2020 року атакувала 168 компаній. У лютому 2024 було затримано двох міжнародних злочинців, а у результаті спільної операції Служби безпеки України, правоохоронних органів США, Великої Британії, Євросоюзу та інших країн-партнерів викрито учасників потужного міжнародного угруповання вимагачів LockBit. У травні 2024 правоохоронні органи 13 країн провели спецоперацію Endgame, яка дозволила знищити кримінальну інфраструктуру ряду зловмисних груп, зокрема IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee і Trickbot. Українські правоохоронці здійснили більшість арештів та обшуків в рамках цієї операції. Також у травні Служба безпеки України та FBI спільно з правоохоронними органами Великої Британії та ЄС провели спецоперацію у восьми країнах Європи, викривши понад 30 учасників транснаціональних хакерських угруповань

РОЗВИТОК МІЖНАРОДНОЇ СПІВПРАЦІ

Україна активно розбудовує міжнародну співпрацю. У листопаді 2023 року Україна (НКЦК при РНБО України та ДССЗЗІ) підписали Робочу угоду про співпрацю з ENISA (Європейською агенцією кібербезпеки). Для ENISA це стало першою такою угодою з партнером з-поза меж ЄС. Підписання таких документів – важливий елемент на шляху формування глобальної кіберкоаліції для протидії загрозам, що походять із росії та інших держав, які стоять по один бік з агресором.

Для стимулювання міжнародної співпраці та взаємодії 7-8 лютого у столиці України відбувся перший Київський міжнародний форум з кібербезпеки 2024: «Стійкість під час кібервійни», започаткований НКЦК України разом з партнерами. Загалом у Форумі взяли участь понад тисяча учасників, серед яких

топ посадовці України, США, ЄС та НАТО. Під час заходу відбулося 10 панельних дискусій і понад 40 експертних доповідей, які розкривали роль кібербезпеки у сучасних війнах, досвід України у кібервійні, тему кібервійни і міжнародного права, кібердипломатії, посилення стійкості національної системи кібербезпеки через освіту, захищеність месенджерів, роль розвідки кіберзагроз, кібербезпека регіонів та інші.

У серпні 2024 року відбулися кілька важливих подій: шостий раунд Кібердіалогу Україна–США (обговорювались питання сучасного ландшафту кіберзагроз, захист критичної інфраструктури, кіберсанкції та кібердипломатія), зустріч представників НКЦК з Посольством Японії та JICA (розглянуто можливість навчання японських колег українськими фахівцями), а також підписання Меморандуму про співпрацю у сфері кібербезпеки та кіберзахисту між Держспецзв'язку та Міністерством оборони Латвії.

ЄВРОПЕЙСЬКА ТА ЄВРОАТЛАНТИЧНА ІНТЕГРАЦІЯ

Україна зосередила увагу на різних аспектах інтеграції до ЄС і НАТО. На першій науково-практичній міжнародній конференції з питань кібердипломатії, яка відбулася в Києві в травні 2024 року за підтримки НКЦК, Міністр закордонних справ Дмитро Кулеба підкреслив, що Україна, завдяки своєму досвіду протидії рф та репутацією новатора, є невід'ємною частиною європейської та євроатлантичної систем безпеки.

На початку травня 2024 Україна провела першу зустріч з представниками ЄС як країна-кандидат, зосереджену на питаннях цифровізації, зокрема на переговорному Розділі 10 «Цифрова трансформація та медіа». Міністерство оборони затвердило «Основні засади інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах», враховуючи найкращі підходи НАТО, міжнародні стандарти та практики з інформаційної та кібербезпеки. На третьому міжнародному засіданні Національного кластера кібербезпеки в Бухаресті у квітні 2024 року було розглянуто питання поглиблення співпраці з ЄС та НАТО та обговорено практичні кроки, які Україна здійснює у сфері кібербезпеки. В липні відбувся третій раунд Кібердіалогу Україна-ЄС, під час якого було досягнуто домовленості про поглиблення співпраці. Йшлося про імплементацію норм європейського законодавства до української правової бази.

ПІДТРИМКА З БОКУ ПАРТНЕРІВ

Протягом звітного періоду партнери України надавали їх значну підтримку у протистоянні російській агресії. В грудні 2023 Естонія та ще 9 держав запустили Талліннський механізм для посилення цивільної кіберпідтримки України. Його мета – систематизувати потреби України та співвідносити їх з можливостями партнерів. Перше засідання Талліннського механізму пройшло у Гаазі у середині лютого 2024 року.

Наразі Україна очікує на 13 мільйонів доларів кібердопомоги від Данії, а USAID допомагає розбудовувати кібербезпеку енергетичного сектору. В липні

IT-коаліція передала Україні мережеве обладнання та ліцензії, що підсилять потужність центрів обробки даних та кіберзахисту Міністерства оборони та Збройних сил України. У вересні до IT-коаліції приєдналася Іспанія, ставши 13-м партнером у цій сфері.

За підтримки партнерів Україна запускає спільні проєкти у сфері кібербезпеки. Це включає інформаційні кампанії з кібергігієни, адаптацію інструментів кібердіагностики (як-от CSET), та впровадження автоматизованих систем для моніторингу реалізації Стратегії кібербезпеки України (CyberTracker).

VII. ПЕРША СВІТОВА КІБЕРВІЙНА

ЗМІНИ У ХАРАКТЕРІ СВІТОВОГО КІБЕРПРОТИСТОЯННЯ

Глобальне кіберпротистояння набирає обертів, залучаючи нових учасників. російсько-українська кібервійна залишається важливим елементом цього протиборства, проте не обмежується лише прямим протистоянням росії та України. Ареал активності політично мотивованих хакерів розширюється. Паралельно з російсько-українським фронтом зростає активність навколо Тайваню, де кіберугруповання, ймовірно пов'язані з КНР, збільшують атаки. США або Ізраїль підозрюють в атаці на Центральний банк Ірану. Активні дії в кіберпросторі демонструють також північнокорейські хакери.

Водночас російські хакери продовжували зберігати активність протягом всього періоду, хоча їх діяльність еволюціонувала. Вони часто синхронізували свої дії з загальною російською військовою стратегією, наприклад, атакуючи паралельно з ракетними ударами сільськогосподарський сектор України. Також APT групи, які працюють проти України, майже не змінюються.

Також російські хакери постійно атакують союзників України, намагаючись знизити рівень їх підтримки. У квітні пройшла хвиля кібератак на муніципальні ресурси в США, міські IT системи та водний сектор США, в яких були виявлені зусилля російських кіберугруповань. Використовуючи звичну тактику, росіяни знайшли найбільш вразливий до кібератак сегмент, нанесення шкоди якому може мати значні соціальні наслідки. Наприкінці 2023 російська APT29 атакувала посольства по всій Європі. Атаки таких угрупувань як Killnet чи Anonymous Sudan проти союзників України в США та Європі були регулярним явищем наприкінці 2023 року.

Міжнародні дослідники зазначають, що росія змінює фокус кібератак з українських організацій на особисті мобільні пристрої військовослужбовців і співробітників сектору безпеки.

Microsoft також стала жертвою атаки російського державного нападника Midnight Blizzard. Обсяги кібервтручання групи Midnight Blizzard все ще не до кінця зрозумілі - наразі Microsoft підтвердила лише, що зловмисники змогли отримати доступ до деяких сховищ її вихідного коду та внутрішніх систем. Атака зачепила і деякі акаунти електронної пошти високопосадовців США, що змусило CISA проводити власне розслідування та вживати заходів для пом'якшення наслідків.

КІБЕРШПИГУНСЬКІ ОПЕРАЦІЇ

Відповідно до даних компанії Microsoft, у 2023 році авторитарні уряди (росії, КНР, Ірану та Північної Кореї) сконцентруватися на кібершпигунських операціях, намагаючись отримати більше інформації щодо важливих для них

зовнішньополітичних ініціатив. Мішенню атак вищезгаданих акторів стають не лише західні компанії та уряди. Як стверджує російська державна компанія “Солар”, Китай і Північна Корея стали ключовими джерелами наступальних кіберкампаній проти росії у 2023 році.

ЗАСТОСУВАННЯ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА У КІБЕРСФЕРІ

Застосуванням міжнародного гуманітарного права до кіберсфери під час війни знаходиться у фокусі уваги України та партнерів. Національний координаційний центр кібербезпеки разом із партнерами обговорює такі питання як статус комбатантів у «кібервійні», міжнародний досвід щодо застосування міжнародного гуманітарного права до проведення кібероперацій, правовий аналіз кібератак, що відбувались під час російсько-української війни тощо.

У червні стало відомо, що прокурори Міжнародного кримінального суду розслідують ймовірні російські кібератаки на українську цивільну інфраструктуру як можливі воєнні злочини. Розслідування охоплює атаки, які поставили під загрозу життя цивільних, порушуючи електропостачання та водопостачання, перериваючи зв’язок зі службами екстреного реагування або виводячи з ладу мобільні служби передачі даних, що передають попередження про повітряний наліт. Служба безпеки України також збирає докази на хакерів, які наприкінці 2023 року атакували оператора мобільного зв’язку «Київстар». Ці матеріали будуть передані до Міжнародного кримінального суду.

РЕКОМЕНДАЦІЇ

ШІ та нові загрози

- Підготувати нормативні документи, що визначають процес відповідального розвитку технологій ШІ в Україні з акцентом на використання ШІ в сфері ІТ, державного управління, виконання завдань сектору безпеки і оборони України (використання ШІ для наступальних та оборонних заходів). Це включатиме і стимулювання навчання використанню ШІ. Варіантом вирішення цього питання є створення державної стратегії з питань впровадження ШІ в кібербезпеку, подібної до документу, затвердженого CISA у січні 2024 року.
- Потрібна цілісна оцінка реальних потреб сектору безпеки і оборони в технологіях ШІ для виконання визначених законодавством завдань. Оцінка має включати не лише перелік потреба, але й очікуваних заходів самих суб'єктів цього сектору які вони планують вжити щодо задоволення цих потреб.
- Підходи Secure by Design та Zero Trust Architecture стають довгостроковими трендами, що можуть значно покращити кібербезпеку. Доцільно оцінити можливість впровадження підходу Secure by Design при розробці програмного забезпечення для державних органів та надання державних послуг.

Кібербезпека на місцевому рівні

- В той час, як кібербезпека центральних органів влади часто забезпечується та підтримується діяльністю ключових кібербезпекових структур України, місцевий рівень традиційно залишається менш захищеним. Доцільно врахувати цей напрямок загального підвищення кібербезпеки країни, в тому числі через розробку спрощених (базових) настанов з кібербезпеки для організацій місцевого значення. Як вказує досвід США та Великобританії, хакери все частіше орієнтуються на такі організації (в тому числі з числа водного сектору) аби завдати практичної шкоди на локальному рівні.
- Для локального рівня доцільно створити більше інструментів самооцінки стану кібербезпеки (наприклад, використовуючи набори рекомендацій CISA Cybersecurity Performance Goals) аби організації мали доступ до найкращих кібербезпекових практик та могли оцінити свій стан самостійно
- Україна майже не має точних знань про стан кібербезпеки місцевих органів влади та їх потреби/можливості в сфері кібербезпеки. Доцільно ініціювати оцінку кібербезпекових потреб організацій місцевого значення з метою подальшого формування цілісної державної політики щодо таких суб'єктів.

Кібербезпека медіа

- Медіаорганізації все частіше стають цілями кібератак. Доцільно провести оцінку захищеності медіаорганізацій в Україні (в т.ч. ліцензіатів Національної ради з питань телебачення і радіомовлення) та надати їм рекомендації щодо можливих шляхів покращення захисту.

Безпека ланцюжків поставок (Supply chain)

- Хоча проблема кібератак через ланцюжки поставок добре відома, кібербезпекові організації по всьому світу продовжують свої зусилля щодо пояснення шляхів пом'якшення таких загроз для різних цільових аудиторій. Це включає загальні настанови щодо того як правильно мають визначатись ланцюжки постачання, перелік ключових заходів пом'якшення загроз та списки рекомендованих матеріалів для додаткового опрацювання. Українські організації також потребують таких адаптованих документів як з метою практичного застосування так і підвищення обізнаності щодо цієї проблеми.

OKI (IT/OT)

- Кібербезпека ОТ інфраструктури ОКІ – один з пріоритетів в умовах триваючої кібервійни. Специфічність цієї сфери потребує створення більш тісних та дієвих шляхів взаємодії у трикутнику держава-бізнес-вендори. Одним з кроків на цьому шляху може стати допомога держави у приєднанні зацікавлених суб'єктів кібербезпеки до вендорських програм підтримки (як, наприклад, програми Dragos) з метою розширення можливостей залучення безкоштовної допомоги в питаннях кібербезпеки ОТ.
- Досвід США в оцінці стану кібербезпеки підприємств окремих секторів критичної інфраструктури, зокрема водного, підкреслює необхідність кращої систематизації таких даних в Україні. Рекомендується запровадити обов'язкову регулярну самооцінку кібербезпеки для всіх об'єктів критичної інформаційної інфраструктури (ОКІ) відповідно до Методики, затвердженої Наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами). Для ОКІ 3-4 категорії можна розглянути спрощену модель самооцінки, наприклад, на основі CISA CPG.
- США вживає все більше заходів спрямованих на посилення кіберзахисту медичного сектору. Зважаючи на високі темпи цифрової трансформації цієї сфери в Україні, доцільним є провести тематичний аналіз стану кіберзахисту українського медичного сектору та оцінити, чи можливі помітні негативні наслідки у випадку кібератаки на організації цієї сфери. Також, незалежно від результатів такого огляду, доцільно було б підготувати набір стандартних (базових) рекомендацій кіберзахисту для їх обов'язкового поширення МОЗ України до всіх організацій медичного сектору.

Кібернавчання: збільшення кіберфахівців

- Навчання нового покоління кіберфахівців є пріоритетом для багатьох країн. В контексті підготовки нового проєкту Стратегії кібербезпеки на період після 2025 року, варто визначити підхід України до цього питання. Доцільно включити це окремим розширеним блоком в оновлену Стратегію кібербезпеки або розробкою окремого документа, наприклад, Стратегії розвитку кадрів у сфері кібербезпеки.
- Україна, як і більшість країн світу, стикається з нестачею кваліфікованих кіберфахівців, передусім в державному секторі, і має так само шукати шляхи вирішення цього питання. Доцільно врахувати досвід США які йдуть шляхом розширення бази навчання за рахунок нових цільових аудиторій (з акцентом

на жінок, військовослужбовців, перекваліфікацію державних службовців) та зміну вимог на посадах для таких фахівців (спрощуючи вимоги).

Міжнародна співпраця

- Міжнародна співпраця та її систематизація все ще потребують помітних зусиль. Протягом 2022-2023 років Україна встановила партнерські відносини з європейською ENISA та американською CISA. Обидві організації мають потужну експертизу в аналізі та дослідженнях (ENISA) та розширенні кіберсервісів для всіх стейкхолдерів (CISA). Аби максимально ефективно використати цю експертизу Україні доцільно створити більш чіткі та деталізовані плани співпраці зі зрозумілими кінцевими цілями.
- Рано чи пізно Україна постане перед питанням виборчого процесу який буде пов'язаний із широким застосуванням ІТ. Вже зараз доцільно активізувати співпрацю з CISA з цих питань, як отримуючи результати їх досвіду забезпечення безпеки виборів, так і запропонувати власну допомогу з забезпеченням кібербезпеку їх виборчого процесу (шляхом інтенсифікації інформаційних обмінів про кіберзагрози).
- В той час як євроінтеграція залишається абсолютним зовнішньополітичним пріоритетом України, цьому процесу (в частині кібербезпеки) потрібна більша систематизація та прозорість. Доцільно більш чітко визначити перелік європейських нормативних актів, які підлягають імплементації/адаптації в Україні та оцінити ступінь виконання цього процесу. Це, також, потребуватиме і регулярного моніторингу законодавчих змін ЄС та надання оцінок щодо можливих часових проміжків для імплементації цих ініціатив в українське законодавство.