УДК 342.951

КРАСНІКОВ С.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-6548-5457.

ШЛЯХИ ПОСИЛЕННЯ СТАНУ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

DOI...

Анотація. *Визначено пріоритетні засади забезпечення кібербезпеки в умовах війни. Проведено аналіз тактики діяльності спецслужб держави-агресора у вказаному контексті. Деталізовано головні тренди кібербезпеки у 2022 році. Визначено складові вітчизняної моделі посилення стану кібербезпеки в умовах війни. Розкрито алгоритм реагування суб'єктами забезпечення кібербезпеки на кіберінциденти та кібератаки. Висвітлено законодавчі та інші нормативні акти, які були схвалені з метою посилення стану кібербезпеки в умовах кібервійни. Присвячена увага положенням Стратегії кібербезпеки України з метою необхідності уточнення її деяких положень в умовах війни. Визначено подальші шляхи удосконалення чинного законодавства з метою посилення стану забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, кіберпростір, хакерські атаки, кіберзлочинці, експлойт, кібердомен, ландшафт кіберзагроз, кібервійна.*

Summary*. The priority principles of ensuring cyber security in the conditions of war have been determined. An analysis of the tactics of the special services of the aggressor country in the specified context was carried out. The main cyber security trends in 2022 are detailed. The components of the domestic model of strengthening the cyber security in the conditions of war were determined. The algorithm for responding to cyber incidents and cyber attacks by cyber security entities has been revealed. The legislative and normative acts that were approved with the aim of strengthening the cyber security in the conditions of cyber war are highlighted. Attention is paid to the provisions of the Cybersecurity Strategy of Ukraine with the aim of clarifying some of its provisions in wartime conditions. The further directions of improving the current legislation in order to strengthen the cyber security have been identified.*

Keywords*: cyber security, cyber attack, cyber space, hacker attacks, cyber criminals, exploit, cyber domain, cyber threat landscape, cyberwar.*

Постановка проблеми. За оцінками світових експертів у сфері кібербезпеки, у переважній більшості країн спостерігається стійка тенденція до значного збільшення кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури. Основними цілями кібератак стають об'єкти стратегічної інфраструктури країн (ядерна, транспортна, хімічна чи будь-яка інша промисловість, системи життєзабезпечення великих мегаполісів, фінансова, продовольча, енергетична національні системи, транспортні мережі, діяльність уряду, правоохоронних органів тощо). Посягання здійснюються через інформаційно-телекомунікаційні системи, особливо автоматизовані системи управління, які необхідні для повсякденного життя людей, функціонування структур економіки, органів державної влади.

Забезпечення належного рівня кібербезпеки складно уявити без чітко спланованих спільних дій та розроблених заходів відповідальних суб'єктів, які мають бути синхронізовані і здійснюватися за єдиним стратегічним задумом й вектором розвитку національної системи кібербезпеки декларативного характеру. Саме тому кібербезпека визнана у більшості країн світу як важлива складова національної безпеки, забезпечення якої неможливе без формування і функціонування загальнодержавної системи у сфері кібербезпеки, яка ґрунтується на таких засадах, як повага до принципів і норм міжнародного права, захист фундаментальних цінностей, визначених чинним законодавством, забезпечення національних інтересів у кіберпросторі. Загальною усталеною практикою країн світу стає чітке доктринальне визначення концептуальних засад державної політики у сфері забезпечення безпеки у кіберпросторі у форматі актів стратегічного планування.

Будь-який стратегічний документ кібербезпекової тематики державного рівня має враховувати не тільки внутрішньополітичні аспекти, але й сучасні світові тренди в глобальному кіберсередовищі як вагомі фактори впливу на розбудову національної системи кібербезпеки будь-якої держави світу. Загальноприйнятим світовим трендом є тотальна кібервійна, а також той факт, що схвалені останнім часом національні стратегії кібербезпеки відображають політичну волю та свідоме прагнення країн світу максимально забезпечити власну кібербезпеку, протидію кіберзлочинності як на національному так і міжнародному рівнях, максимально запобігти несанкціонованому витоку даних та конфіденційної інформації, адекватно реагувати на виклики та загрози у кібердомені.

Прогнозування розвитку безпекового середовища навколо України на період до 2025 року демонструє, що суб'єктам забезпечення національної безпеки держави необхідно було запроваджувати заходи для захисту національних інтересів в інформаційному просторі, невід'ємною частиною якого є саме домен кіберпростору.

Проте ситуація навколо кібербезпеки України кардинально змінилася після 24 лютого 2022 року. Одночасно розпочалася перша у світі кібервійна, яка ніколи не закінчиться у кібердомені. З початку війни Україна стала об'єктом чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також перебувають у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетами у війні. Таким чином, продовжується тривала боротьба з державою-агресором на кіберфронті, який працює у режимі 24/7. Крім виявлення та запобігання кібератакам на українські ресурси, правоохоронні органи та кібердобровольці надають гідну відсіч супротивнику: щотижня атакують більше сотні онлайн-ресурсів, пов'язаних з рф та їхніми сервісами для бізнесу; здійснюють DDoS-атаки, які призводять до блокування роботи та збою в інформаційних системах росЗМІ; іноді зупиняють деякі підприємства військово-промислового комплексу.

Таким чином, в умовах війни актуальним питанням є посилення стану кібербезпеки, що у свою чергу, потребує проведення наукових досліджень з метою визначення ключових завдань у цій площині.

Результати аналізу наукових публікацій. Організаційно-правові проблеми забезпечення кібербезпеки в Україні та за кордоном досліджували у своїх наукових працях А. Баранов [1], М. Гребенюк [2], І. Доронін [3], І. Діордиця [4], О. Кузнєцов [5] та ін. Питання інституційного становлення та розбудови національної системи кібербезпеки розглядали С. Гуржій [6], В. Петров [7], А. Тарасюк [8], Н. Ткачук [9].

Проте сьогодні бракує предметних досліджень із забезпечення кібербезпеки в умовах воєнного стану, що засвідчує актуальність обраної теми наукової статті.

Метою статті є визначення на базі узагальнення законодавчих новел й ініціатив у сфері забезпечення кібербезпеки, перспективних та дієвих заходів, спрямованих на посилення стану забезпечення кібербезпеки в умовах кібервійни.

Виклад основного матеріалу. Ще до повномасштабного вторгнення росії в лютому 2022 року експерти з кібербезпеки готувалися до можливих кібератак як в Україні, так і в країнах-союзниках. Адже рф робила це і раніше: вірус NotPetya, який завдав суттєвої шкоди в 2017 році приписують саме російським хакерам. Зловмисне програмне забезпечення, яке також поширилося далеко за межами України, блокувало файли у спосіб, подібний до програм-вимагачів. Проте, коли експерти розібралися детальніше, вони зрозуміли, що справжньою метою було знищити дані, а не заробити гроші.

Війна в Україні стала каталізатором глобального розвитку кіберзахисту та необхідності посилення кібербезпеки у світі. Війна ведеться як на полі бою, так і в кіберпросторі. Потужність українських кібервійськ визнають у всьому світі. При цьому армія українських хакерів викликає захоплення і повагу. Бо міжнародна спільнота спостерігає за абсолютно новим рівнем кіберзагроз, який не має аналогів у минулому. По суті, зараз відбувається перша у світі цифрова війна, на хід якої безпосередньо впливають високі технології. У 2022 році рф втричі збільшила кількість кібератак на Україну. Вони переважно спрямовані на цивільну інфраструктуру, зокрема, енергетичну та логістичну, а також на державні реєстри. Зокрема, фіксується активізація використання спецслужбами рф підконтрольних хакерських угруповань для здійснення протиправного кібервпливу на державні електронні інформаційні ресурси та критичну інформаційну інфраструктуру України з метою реалізації актів кібершпигунства, кібертероризму, а також у якості інструментарію спеціальних інформаційних операцій.

Аналіз тактики діяльності спецслужб держави-агресора дозволяє стверджувати, що основною формою проведення протиправного кібервпливу є цілеспрямовані довгострокові кібероперації (APT-атаки), які реалізовуватимуться шляхом застосування моделі *cyber kill-chain*. Вказана модель передбачає проведення кібератак у кілька етапів, причому інструментарій та тактика кожного наступного етапу залежить від результатів попереднього та характеру існуючих вразливостей системи. Зокрема, до таких етапів належать: сканування системи з метою виявлення її вразливостей; застосування спеціального програмного забезпечення (експлойту) або методів соціальної інженерії для проникнення в систему; інсталяція шкідливого програмного забезпечення (далі – ШПЗ) для віддаленого управління системою; безпосередня крадіжка або модифікація даних, блокування роботи системи тощо. На кінцевому етапі зловмисниками вживаються заходи, спрямовані на знищення слідів своєї протиправної діяльності. З метою реалізації вказаних кіберзагроз російськими спецслужбами на постійній основі залучаються такі хакерські угруповання, як: APT28 (Sofacy, Sednit, FancyBear), Turla (Waterbug та White Bear), а також APT29 (Cozy Bear та The Dukes) тощо.

На сьогодні ризики кібератак з боку рф як на українські системи, так і на європейських партнерів залишаються досить високими. Кібербезпека наразі є ключовим та стратегічним питанням в економічному, політичному, соціальному та військовому аспектах. Перед вітчизняними правоохоронними органами та кібердобровольцями постає все більше завдань з пошуку нових засобів та методів дієвої боротьби з кіберзлочинністю та кібертероризмом. Для вітчизняного сегменту кіберпростору небезпечною та загрозливою залишається діяльність спецслужб рф та хакерських

угруповань, які скоюють чисельні кібератаки. Актуальним питанням залишається налагодження плідної взаємодії державних та недержавних установ у питанні забезпечення кібербезпеки критичної інфраструктури України в період воєнного стану.

На цьому фоні можливо визначити головні тренди кібербезпеки у 2022 році:

1) розширення спектру поверхневих атак. Нині 60 % офісних співробітників працюють віддалено, і принаймні 18 % не повернуться в офіс. Враховуючи широке використання "хмари", рішень з відкритим кодом, часту взаємодію із "зовнішнім світом" у вигляді соцмереж, з'являються нові та складні "поверхні атак", тобто зростає число джерел ризиків, що робить державні та комерційні організації більш вразливими до кібератак. У зв'язку з цим керівникам безпеки в організаціях та установах було наполегливо рекомендовано виходити за рамки традиційних підходів до моніторингу кібербезпеки, виявлення та реагування на кіберзагрози;

2) необхідність стабільного посилення захисту систем ідентифікації, оскільки саме ці системи піддаються постійним кібератакам та залишаються уразливими. Зловживання обліковими даними тепер є основним методом, який хакери та зловмисники використовують для доступу до систем і досягнення своїх цілей. Наприклад, у зламі SolarWinds зловмисники використовували привілейований доступ постачальника для проникнення в цільову мережу;

3) збільшення ризиків при постачанні ПЗ. Прогнозується, що до 2025 року 45 % організацій у всьому світі зазнають атак на свої ланцюжки поставок програмного забезпечення, що в три рази більше, ніж у 2021 році. Це нова стратегія зловмисників, адже ламати програмне забезпечення простіше у момент його створення, особливо під час використання розробниками загальнодоступних бібліотек. У зв'язку з цим керівники безпеки та управління ризиками повинні контролювати усі етапи постачання ПЗ для того, щоб не допустити вразливостей систем. Тобто загрозу становлять не лише прямі дії хакерів-злочинців, а й зараження техніки вірусами, збої у роботі програмного забезпечення та несанкціонований доступ до нього, що зумовлює потребу комплексного підходу до питань забезпечення кібербезпеки та захисту інформації.

У зв'язку зі збільшенням кількості та масштабу кібернападів як одного із проявів агресії рф проти України, що спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України, а також об'єкти критичної інформаційної інфраструктури, набуває актуальності питання вдосконалення нормативного забезпечення питань кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, а також об'єктів критичної інформаційної інфраструктури. Триваюча війна з рф спричинила зміни в "ландшафті кіберзагроз" в Україні, оскільки кібератаки проти України за останній рік зросли втричі, причому онлайн-атаки іноді поєднуються з ракетними ударами. Отже, з початку військової агресії рф проти України кількість кібератак на Україну суттєво зросла, не дивлячись на те, що українці не перший рік активно протидіють ворогу в кіберпросторі. Проте у світі, на жаль, досі не існує уніфікованого нормативного визначення поняття "кібервійна". Наслідком відсутності нормативно-правової бази є неможливість формування адекватних сил і засобів реагування на наявні ризики та загрози. Складним залишається і питання швидкого притягнення винних до відповідальності за військові злочини в кіберсфері.

На це звертають увагу П. Горінов та Р. Драпушко, які констатують, що транскордонний характер кіберпростору, його залежність від складних інформаційних технологій, активне використання сайтів і сервісів кіберпростору всіма верствами населення виявляють нові можливості, але також викликають нові загрози, в тому числі:

а) шкоду правам, інтересам і життю окремих осіб, організацій, державних установ; б) кібертероризм; в) використання кіберзброї на війні; г) кібервійни, в тому числі ті, які супроводжують традиційну ворожнечу. Незважаючи на всі публічні заклики до мирного використання кіберпростору в інтересах всіх людей і націй, уряди багатьох провідних країн активно включилися в гонку кіберзброєння, відтворюючи класичну "дилему безпеки" на якісно новій основі. Це означає, що на тлі складних і суперечливих глобальних процесів політичного, економічного і соціального розвитку кіберпростір стає простором холодної війни, тобто основою нового протистояння (переважно в кіберпросторі) ключових геополітичних акторів [10, с. 268].

Проте Україна формує власну модель посилення стану кібербезпеки в умовах війни, що потребує, у першу чергу, прискорення розробки та схвалення відповідних нормативних актів, які відповідають умовам сьогодення. На початку квітня 2023 року Кабінет Міністрів України видав постанову, яка визначає процедуру реагування на кіберінциденти та кібератаки. Нова постанова Уряду України дозволить вчасно реагувати та планувати заходи з кіберзахисту. Мова йде про Постанову Кабінету Міністрів України від 04.04.23 р. № 299 "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" [11]. Цією постановою затверджено Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Нормативно встановлено, що реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту.

Алгоритм реагування суб'єктами забезпечення кібербезпеки на кіберінциденти/ кібератаки розпочинається з етапу підготовки, під час якого здійснюються заходи з дослідження сучасних видів кіберінцидентів/кібератак, розроблення методів і механізмів запобігання та протидії можливим кіберінцидентам/кібератакам. На етапі виявлення та аналізу суб'єкти забезпечення кібербезпеки здійснюють виявлення кіберінциденту/ кібератаки та визначають їх критичність для забезпечення пропорційності та/або співрозмірності подальших заходів з кіберзахисту реальним та потенційним ризикам.

Суб'єкти забезпечення кібербезпеки визначають критичність кіберінциденту/ кібератаки відповідно до методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв'язку України, за такими 5 категоріями (рівнями):

рівень 0, некритичний (білий) – кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем;

рівень 1, низький (зелений) – кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються;

рівень 2, середній (жовтий) – кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і

доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою;

рівень 3, високий (помаранчевий) – кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб'єкта національної системи кібербезпеки;

рівень 4, критичний (червоний) – кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки;

рівень 5, надзвичайний (чорний) – кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

Під час етапу стримування суб'єктами забезпечення кібербезпеки вживаються заходи до зниження негативного впливу кіберінциденту/кібератаки, запобігання порушенню безпеки, забезпечення сталого, надійного та штатного режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, несанкціонованого втручання в їх роботу, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

За результатами вжиття заходів до кіберзахисту суб'єкти забезпечення кібербезпеки проводять аналіз ефективності реагування на кіберінциденти/кібератаки. Під час цього етапу забезпечується вивчення задокументованих даних щодо кіберінциденту/кібератаки, інформування керівництва суб'єкта забезпечення кібербезпеки, узагальнення та проведення аналізу досвіду реагування для подальшого підвищення ефективності вжиття заходів до кіберзахисту у разі можливих кіберінцидентів/кібератак у подальшому.

Узагальнюючи викладене, можна констатувати, що визначений порядок у новій процедурі реагування дасть змогу: швидко виявити та захиститися від кіберінцидентів чи кібератак; повідомити про небезпеку, запобігти негативним наслідкам чи мінімізувати їх; виявити і виправити вразливості; відновити сталість і надійність функціонування інформаційних, електронних комунікаційних, інформаційно-

комунікаційних, технологічних систем та інших об’єктів кіберзахисту. Процедура реагування на кібератаки та кіберінциденти складається з декількох етапів: підготовка, виявлення й аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування. Також постанова визначає критичність кібератак та кіберінцидентів.

Ця постанова була розроблена Державною службою спеціального зв’язку та захисту інформації України на виконання Плану реалізації Стратегії кібербезпеки України на 2023 рік. У останньому звіті Держспецзв’язку України вказує, що російські хакери замість атаки на організації-цілі за допомогою фішингу та шкідливого програмного забезпечення почали зміщувати акцент на використання технічних вразливостей організацій та установ, які надають послуги операторам критичної інформаційної інфраструктури, зокрема розробників та Інтернет-провайдерів.

Окрім зазначеної постанови у 2022 році була ухвалена низка важливих законів та підзаконних актів, зокрема законодавчі зміни стосуються активної протидії агресії у кіберпросторі [12], Хмарних послуг та розміщення у “хмарах” державних інформаційних ресурсів [13], посилення захисту критичної інфраструктури України [14], регламентований механізм забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану [15] тощо.

Також в Україні діє Стратегія забезпечення кібербезпеки, яка була введена в дію рішенням РНБО України від 14 травня 2021 року [16]. Стратегія кібербезпеки України була розрахована до 2025 року як фундаментальний документ національного значення, який регламентує вектор щодо подальших кроків розбудови національної системи кібербезпеки в нашій державі, системних заходів щодо надійного захисту національного сегменту кіберпростору, зовнішньополітичної діяльності у сфері посилення кібербезпеки тощо. Загалом Стратегія кібербезпеки України складається з дев’яти взамопов’язаних розділів та детально визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення передумов задля побудови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Стратегія кібербезпеки України враховує попередній досвід і проблеми, поточний та перспективний стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО. 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. У цій Стратегії 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. У положеннях Стратегії наголошується, що саме кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Окреслено тенденцію зі створення власних кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі. У тексті Стратегії саме рф визначена основним джерелом загроз національній та міжнародній кібербезпеці. Враховуючи масштаби військової агресії рф проти України, вважаємо, що деякі положення вказаної Стратегії мають бути уточнені, оскільки не повною мірою відображають реальний стан справ у сфері кібербезпеки сучасності.

Зокрема, важливим завданням держави в умовах воєнного стану залишається: створення та оптимізація ефективної національної системи кібербезпеки, з урахуванням тенденцій динаміки зміни безпекового середовища та кращих практик у сфері кібербезпеки провідних країн світу; набуття суб'єктами забезпечення кібербезпеки необхідних спроможностей для виконання оперативних завдань у кібердомені за призначенням; створення передумов для опанування сучасних форм та способів підготовки та проведення заходів забезпечення кібербезпеки; нарощування потужностей щодо підготовки та ведення кібербезпеки (у т. ч. кіберзахисту, кібероборони) відповідно до зростання рівня кіберзагроз; вчасне реагування на поточні загрози кібербезпеки шляхом запобігання, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу; створення ефективних систем управління для забезпечення кібербезпеки; налагодження ефективної співпраці у межах повноважень із суб'єктами забезпечення національної безпеки держави, а також з НАТО, ЄС, державами-партнерами в частині спільного виконання завдань кібербезпеки.

У березні 2023 року Держспецзв'язку презентовала аналітичний звіт про кіберагресію росії проти України у 2022 році "Russia's Cyber Tactics: Lessons Learned 2022" [17]. За результатами, оприлюдненими Держспецзв'язку, можна констатувати основні тенденції та про динаміку російської кіберзагрози. Кібератаки – повноцінна складова російської війни проти України. Цілі, які стоять перед російськими хакерами, відповідають загальним цілям російської воєнної агресії. Основною метою російських кіберзлочинців є цивільна інфраструктура, а пріоритети хакерів упродовж повномасштабного вторгнення змінювалися відповідно до воєнних потреб. Хоча державні структури постійно залишалися ключовими цілями кібератак, на початку вторгнення важливими об'єктами атак були медіа та телеком, оскільки російська влада розраховувала на швидку перемогу і сподівалась, що зможе вплинути та налякати українців через ЗМІ.

Згодом фокус хакерів і російської армії змістився на енергетичний сектор. Таргетований фішинг залишається одним із домінантних і ефективних методів отримання доступу до організацій-жертв. Однак у другій половині 2022 року помітними стали зміни в тактиці російських хакерів. Замість того щоб атакувати безпосередньо організації-цілі за допомогою фішингу, хакери почали зміщувати акцент на використання технічних вразливостей установ, які надають послуги операторам критичної інформаційної інфраструктури. Характер атак російських хакерів вказує на те, що жодна установа не може бути в безпеці. Передусім у зоні ризику – компанії, які надають послуги та сервіси операторам критичної інформаційної інфраструктури: розробники, Інтернет-провайдери тощо. Найбільш небезпечні – російські хакери, що проводять "тихі" операції. Російські хакери здійснюють кібератаки у тому числі з метою помсти або спроб інформаційно-психологічного впливу – щоб переконати населення в тому, що держава не здатна їх захистити. Саме такі атаки привертають до себе увагу ЗМІ та суспільства. Проте насправді більш небезпечними є повільні та "тихі" атаки, спрямовані на шпигунство. Зокрема, такі атаки здійснює угрупування InvisiMole (служба зовнішньої розвідки рф). Їхньою основною ціллю є високопосадовці, дипломати та інші фахівці, які мають доступ до найбільш чутливої інформації. Оскільки такі "тихі" атаки складніше виявити, вони можуть мати більш критичні наслідки.

Переймається проблематикою посилення стану забезпечення кібербезпеки й стратегічний партнер України – США. У лютому 2023 року політичним естаблішментом цієї країни заявлено про виділення $60 млн. на зміцнення кібербезпеки України. Це має допомогти Уряду України захистити об'єкти критичної інфраструктури від російських кібератак. Зокрема, енергетичну, телекомунікаційну та системи зберігання даних [18].

Враховуючи загальносвітові загрозливі тенденції та виклики, пов'язані із збройною військовою агресією рф проти України, у США 2 березня 2023 року було оприлюднено нову національну стратегію кібербезпеки. Цей стратегічний документ чітко формулює мету та завдання, вирішення яких надасть приватним особам, державним структурам та бізнесу можливість консолідовано діяти в цифровій сфері з мінімальними ризиками. Визначено, що США позиціонує себе як надійний партнер розбудови глобальної цифрової екосистеми кібербезпеки, готовий та відкритий для співпраці та взаємодії. Стратегія декларує необхідність здійснити перебалансування відповідальності щодо посилення захисту кіберпростору, переклавши при цьому тягар забезпечення кібербезпеки з окремих осіб, малих підприємств і органів місцевого самоврядування на технологічні корпорації та компанії, які мають найбільші спроможності й найкращі рейтингові позиції. Перспективами розвитку цифрового простору вбачаються динамічні зміни та стимулювання розвитку американської IT-галузі на користь довгострокових інвестицій, дотримання балансу між захистом від нагальних загроз сьогодні та одночасним стратегічним плануванням й інвестуванням у стійке цифрове майбутнє. Досягнення загальних цілей вимагає розвиток глобального кіберпростору, у якому від держав очікується відповідальне ставлення до процесів посилення стану кібербезпеки, а безвідповідальна поведінка може призвести до суттєвих витрат та ізоляції.

Таким чином, положення національної стратегії кібербезпеки США передбачають два фундаментальних аспекти: перерозподіл сфер відповідальності у сфері захисту кіберпростору та переорієнтування стимулів на користь довгострокових інвестицій у кібербезпеку. Цим важливим документом регламентовано напрямки подальшого забезпечення цифрового майбутнього американців. Очікується, що практична реалізація Стратегії дозволить створити міцну основу подальшої розбудови складових інфраструктури кібербезпеки. Фундаментальним моментом є визнання Стратегією того факту, що національний сегмент кіберпростору існує не як самоціль, а формат інструментарію для вирішення питань забезпечення кібербезпеки, виходячи із переліку загроз та викликів сьогодення, реалізації прагнень та задекларованих пріоритетів [20].

Висновки.

Військова збройна агресія рф проти України та цифрова війна у кібердомені вносять свої корективи у світову модель побудови міжнародної безпеки. На цьому фоні дедалі більше держав світу переймаються питаннями посилення стану забезпечення кібербезпеки, що зумовлює уточнення задекларованих стратегічних завдань у цій сфері. З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають перебувати у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни.

Враховуючи ситуацію на міжнародній арені та постійне вдосконалення навичок російських кіберзлочинців та хакерів, на державному рівні необхідно приділяти достатньо уваги питанням посилення стану кібербезпеки та захисту даних. Стійкість системи проти зламів та атак є важливою у будь-якій сфері. Цифрова безпека – тренд останніх років – не втратить своєї актуальності і в 2023-му році. Держава робить важливі кроки з посилення стану забезпечення кібербезпеки як на нормативному, так і методичному рівнях. Така системна робота дозволить врегулювати питання реагування на різні види подій у кіберпросторі, значно посилити захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. З метою забезпечення кібербезпеки України необхідно посилювати взаємодію між основними суб'єктами

національної системи кібербезпеки України, налагоджувати конструктивне і паритетне співробітництво. Посилення стану забезпечення кібербезпеки також передбачає: підготовку та виконання Плану заходів із реалізації Стратегії кібербезпеки на 2023 рік; впровадження та адаптацію законодавства ЄС у національні стандарти у сфері кібербезпеки.

Все ще проблемними питаннями залишаються: не достатня імплементація у чинне законодавство положень Конвенції Ради Європи про кіберзлочинність щодо обов'язкового зберігання та надання на вимогу правоохоронних органів операторами та провайдерами телекомунікацій інформації, необхідної для розслідування кіберзлочинів; використання провайдерами телекомунікаційних послуг механізму перетворення мережевих адрес за технологією NAT (Network Address Translation) без застосування механізмів логування, що ускладнює процес ідентифікації абонентів; використання зловмисниками Інтернет-сервісів та цифрових технологій, а також окремих послуг, що надають провайдери телекомунікацій та хостери, які унеможливлюють ідентифікацію злочинця або ускладнюють отримання іншої інформації, необхідної для розкриття злочину (використання методів TOR та I2P, криптовалют, виділених комунікаційних серверів, т.зв. "куленепробивних хостингів" тощо).

Також важливим є прискорення прийняття законопроекту "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" від 29.09.22 р. № 8087 [19], що надасть змогу посилити стан захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Використана література

1. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика.* № 2(42)/2014. С. 54-62.

2. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право.* 2019. № 2. С. 203-207.

3. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* № 1(20)/2017. С. 106-111.

4. Діордиця І.В. Напрями державної політики кібербезпеки. *Прикарпатський юридичний вісник.* 2017. № 3. С. 111-117.

5. Кузнєцов О.М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. *Інформація і право.* № 1(36)/2021. С. 106-113.

6. Гуржій С.В. Засади інституційно-функціонального забезпечення кібербезпеки в сучасних умовах. *Інформація і право.* № 2(37)/2021. С. 103-114.

7. Петров В.В. Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети.* 2013. № 4 (29). С.127-130.

8. Тарасюк А. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights.* 2020. № 1. С. 167-172.

9. Ткачук Н. Стан та проблемні питання реалізації стратегії кібербезпеки України. *Інформація і право.* № 1(28)/2019. С. 129-134.

10. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2023. № 1. С. 267-270.

11. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text

12. Про внесення змін до Закону України “Про Державну службу спеціального зв’язку та захисту інформації України” щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі: Закон України від 28.07.22 р. № 2470. URL: https://zakon.rada.gov.ua/laws/show/2470-20#Text

13. Про хмарні послуги: Закон України від 17.02.22 р. № 2075. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text

14. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.22 р. № 2684. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text

15. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.22 р. № 263. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

17. Russia’s Cyber Tactics: Lessons Learned 2022. – (Аналітичний звіт Держспецзв’язку про рік повномасштабної кібервійни росії проти України). URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53466

18. Агентство США з міжнародного розвитку (USAID) надасть Україні 60 млн. доларів на зміцнення кібербезпеки. URL: https://www.ukrinform.ua/rubric-economy/3668574-usaid-vidilit-60-miljoniv-na-posilenna-kiberbezpeki-ukraini.html

19. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури: проект закону України від 29.09.22 р. № 8087. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40553

20. National Cybersecurity Strategy. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~