УДК 342.951

ГРІБОЄДОВ С.М., головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0001-6389-0803.

УДОСКОНАЛЕННЯ ДЕРЖАВНОГО ПЛАНУВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Анотація. *Розглянуто засади державного стратегічного планування у сфері забезпечення кібербезпеки. Визначено шляхи удосконалення державного управління у сфері кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів. Проаналізовано та узагальнено недоліки Стратегії кібербезпеки України 2016 року. Розглянуто проєкт Стратегії кібербезпеки України на 2021 – 2025 роки та запропоновано напрями її удосконалення. Окреслено перспективи стратегічного державного планування у сфері забезпечення кібербезпеки в умовах поширення гібридних загроз.*

Ключові слова: *стратегічне планування, державне управління, кібербезпека, кіберзахист, організована кіберзлочинність, кібератака, кіберзагроза, цифрові технології, цифровий суверенітет.*

Summary.*The main principles of state strategic planning in the sphere of cybersecurity are considered. The directions of improvement of public administration in the field of cyber protection of a critical information infrastructure and state information resources are identified. The shortcomings of the Cyber Security Strategy of Ukraine in 2016 are analyzed and summarized. The draft of Cyber Security Strategy of Ukraine for 2021 – 2025 is considered and directions for its improvement are proposed. The prospects of strategic state planning in the sphere of cybersecurity in the context of the spread of hybrid threats are outlined.*

Keywords: *strategic planning, public administration, cybersecurity, cyberdefense, organized crime, cyberattack, cyberthreat, digital technologies, digital sovereignty.*

Аннотация. *Рассмотрены основы государственного стратегического планирования в сфере обеспечения кибербезопасности. Определены направления государственного управления в сфере киберзащиты критической информационной инфраструктуры, государственных информационных ресурсов. Проанализированы и обобщены недостатки Стратегии кибербезопасности Украины 2016 года. Рассмотрен проект Стратегии кибербезопасности Украины на 2021 – 2025 года и предложены направления его усовершенствования. Определены перспективы стратегического государственного планирования в сфере обеспечения кибербезопасности в условиях распространения гибридных угроз.*

Ключевые слова: *стратегическое планирование, государственное управление, кибербезопасность, киберзащита, организованная преступность, кибератака, киберугроза, цифровые технологии, цифровой суверенитет.*

Постановка проблеми. Побудова інформаційного суспільства в різних державах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя, з одного боку створюють підґрунтя для ефективного соціально-економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління. З іншого – перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів надзвичайно вразливими для

реалізації кібернетичних загроз. З огляду на це, функціонування національної системи кібербезпеки унеможливлюється без стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та забезпечення надійного кіберзахисту.

Державне стратегічне планування у сфері забезпечення кібербезпеки залишається важливою складовою реалізації державної безпекової політики виходячи із викликів та загроз в умовах поширення гібридних методів впливу. Саме завдяки державному стратегічному плануванню підвищується ефективність державного управління, визначаються необхідні планові поточні та перспективні заходи, реалізація яких дає змогу мінімізувати внутрішні й зовнішні кіберзагрози, визначати напрями комплексної взаємодії та спільних дій відповідальних суб'єктів забезпечення кібербезпеки. За таких умов державне стратегічне планування у сфері забезпечення кібербезпеки постає важливою складовою політики національної безпеки, виходячи положень Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.20 р. [1].

Стаття 25 Закону України "Про національну безпеку" від 21.06.18 р. [2] визначає засади планування у сферах національної безпеки і оборони, які встановлюються з метою забезпечення реалізації державної політики у цих сферах шляхом розроблення стратегій, концепцій, програм, планів розвитку органів сектору безпеки і оборони, управління ресурсами та ефективного їх розподілу. Планування у сферах національної безпеки і оборони поділяється на довгострокове (понад п'ять років), середньострокове (до п'яти років) та короткострокове (до трьох років). Нормативно встановлено, що одним із документів довгострокового планування виступає саме Стратегія кібербезпеки України. Адже існуюча Стратегія кібербезпеки України потребує перегляду та ухвалення її у новій редакції, виходячи із динамічних цифрових трансформацій та глобальних викликів сучасності, особливо щодо поширення у кіберпросторі гібридних загроз, появи нових форм організованої кіберзлочинності.

Результати аналізу наукових публікацій. Державне планування у сфері забезпечення кібербезпеки як важливу функцію державного управління розглядали у своїх наукових працях такі вчені як: В. Гурковський, О. Заярний, Р. Лук'янчук, А. Семенченко, О. Твердохліб, та ін. Організаційно-правовий аспект цих процесів досліджували: М. Гуцалюк, О. Довгань, Д. Дубов, І. Діордиця, Н. Ткачук.

Проте, у зв'язку із поширенням нових кіберзагроз гібридного характеру, постійного удосконалення цифрових технологій та їх проникнення у всі сфери життя суспільства ці питання потребують подальшого дослідження та ретельного вивчення як науково-теоретичної проблеми.

Метою статті є визначення на базі аналізу сучасних викликів та загроз у кіберпросторі шляхів удосконалення засад державного планування під час підготовки Стратегії кібербезпеки України з урахуванням запроваджених реформ складових сектору безпеки і оборони України

Виклад основного матеріалу. Світовий досвід переконливо засвідчує, що процес забезпечення кібербезпеки в обов'язковому порядку передбачає створення цілісної її системи, яка включає організаційно-правові, фінансові, технічні та оперативні заходи, спрямовані на створення надійного і дієвого кіберзахисту з використанням сучасних методів прогнозування, аналізу, моніторингу й моделювання ситуацій. З метою практичного виконання завдань з реалізації курсу України на європейську та євроатлантичну інтеграцію, впровадження в систему планування єдиних процедур та правил, необхідних для підвищення ефективності сектору безпеки і оборони, для нейтралізації реальних та потенційних загроз національній безпеці України Указом

Президента України від 16.05.19 р. № 225 було введено в дію рішення РНБО України "Про організацію планування в секторі безпеки і оборони України" [3], яким передбачалася підготовка: оборонного огляду; огляду громадської безпеки та цивільного захисту; огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом тощо.

З огляду на актуальність стратегічного завдання держави у сфері забезпечення кібербезпеки у 2019 році було заплановано підготовку Огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів. Ретельний аналіз зазначеного рішення РНБО України дає змогу констатувати, що результатами підготовки вказаного огляду мали стати висновки щодо оцінки безпекового середовища на середньострокову перспективу на глобальному, регіональному та національному рівнях, а також оприлюднена інформація про досягнення стратегічних цілей за результатами проведення заходів реформування сектору безпеки і оборони, оцінку стану підпорядкованих структур сектору безпеки і оборони.

Лише Постановою Кабінету Міністрів України від 11.11.20 р. № 1176 [4] було затверджено порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дозволило нормативно визначити відповідний алгоритм. Метою проведення цього огляду є оцінювання стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, та визначення готовності відповідальних підрозділів суб'єктів, до повноважень яких належить забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури. За результатами огляду визначаються напрями вдосконалення і розвитку національної системи кібербезпеки в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі та фінансово-економічних можливостей держави. Проте, жодних строків щодо проведення вказаного огляду нормативно не встановлено.

Загальновідомо, що державне стратегічне планування завершується розробкою плану дій, який стає початком стратегічного управління, яке умовно можливо поділити на управління функціонуванням та управління розвитком системи забезпечення кібербезпеки. При цьому головними напрямами державного стратегічного планування у сфері забезпечення кібербезпеки можна визначити такі: формування та розвиток системи стратегічного планування забезпечення кібербезпеки; визначення повноважень суб'єктів забезпечення кібербезпеки, у тому числі в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період; посилення прогностичної функції системи управління кібернетичною безпекою (стратегічний прогноз); підвищення ефективності моніторингу у сфері забезпечення кібербезпеки для своєчасного виявлення існуючих і нових типів внутрішніх і зовнішніх кіберзагроз, розробки дієвих заходів щодо їх нейтралізації та блокування; інформаційно-аналітичне забезпечення суб'єктів кібербезпеки; оцінка кібербезпеки, що потребує підготовки галузевих індикаторів її стану; визначення переліку об'єктів та порядку віднесення таких об'єктів до критичної інформаційної інфраструктури; нормативно-правове регулювання зазначеної сфери.

Саме стратегічне планування у сфері забезпечення кібербезпеки дає змогу підвищити ефективність та якість державного управління в зазначеному форматі. Стратегічне планування повинно розглядатися усіма органами державної влади, відповідальними складовими сектору безпеки і оборони України, як універсальний

інструмент, завдяки якому можливо забезпечити реалізацію актуальних державних завдань у сфері забезпечення кібербезпеки, у тому числі й з використанням механізму державно-приватного партнерства. Більш того, як демонструє практика, відмова від державного стратегічного планування у важливих сферах життєдіяльності держави має ризики кризових проявів та негативних наслідків для розвитку суспільства та державних інституцій. Підвищення стратегічних спроможностей Уряду України та відповідальних за забезпечення кібербезпеки правоохоронних та інших державних органів потребує запровадження інституційних засад і стандартів системи стратегічного управління у сфері забезпечення кібербезпеки. Виходячи з аналізу положень Стратегії кібербезпеки України, реалізація заходів, спрямованих на її забезпечення, має здійснюватися чітко на планових засадах та з визначенням конкретних строків.

На жаль, все ще спостерігається висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею. Відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і незадекларованих функцій у такому обладнанні та звужують вітчизняні спроможності протидії кіберзагрозам.

За таких умов планування у сфері безпеки і оборони є важливим та стратегічним завданням держави, сферою відповідальності РНБО України. Оскільки Стратегія кібербезпеки України 2016 року [5] фізично та функціонально застаріла, не відповідає сучасним гібридним викликам та загрозам, то 12 жовтня 2020 року Президент України доручив Національному координаційному центру кібербезпеки розробити проект Стратегії кібербезпеки України та подати його у шестимісячний строк на розгляд РНБО України. З цією метою РНБО України було утворено робочу групу, до складу якої увійшли представники основних суб'єктів національної системи кібербезпеки, Верховної Ради України, Офісу Президента України, Секретаріату Кабінету Міністрів України, Міненерго, Мінінфраструктури, Національного інституту стратегічних досліджень. Основою для розроблення цього програмного документу стали, насамперед, Стратегія національної безпеки України [1], затверджена Указом Президента України від 14.09.20 р., прагнення посилити захист державних інтересів у кібернетичному просторі, адаптувати та впроваджувати кращі практики європейського та міжнародного досвіду у сфері забезпечення кібербезпеки.

Аналіз положень Стратегії кібербезпеки України 2016 року та досвід її практичного впровадження надав змогу сформулювати проблемні питання, які або ускладнювали, або унеможливлювали її ефективну її реалізацію. Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Незадовільним був рівень планування заходів з реалізації Стратегії, заплановані заходи не завжди корелювались із завданнями Стратегії. Об'єктивно, реалізація Стратегії кібербезпеки України 2016 року була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення. Не були розроблені критерії оцінки стану кібербезпеки – індикатори виконання Стратегії, що ускладнило процес моніторингу її результативності та

виокремлення незавершених завдань. Участь у реалізації Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучались інші міністерства і відомства, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучались освітні установи та наукові заклади. Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства.

Нова Стратегія кібербезпеки України має враховувати цей досвід і проблеми та визначити механізми реалізації Стратегії на наступний п'ятирічний період. Стратегія є основою для розроблення інших нормативно-правових актів у сфері кібербезпеки України, а також для обґрунтування розподілу необхідних матеріальних, кадрових та інших ресурсів. Позитивним та прогресивним здобутком політикуму нашої держави стало схвалення проекту Стратегії кібербезпеки України на 2021 – 2025 роки [6], яка була представлена робочою групою при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони України на початку березня 2021 року.

У положеннях проекту Стратегії кібербезпеки знайшли своє відображення концептуальні методологічні підходи до подальшого розвитку й удосконалення національної системи кібербезпеки, які базуються на таких пріоритетах: всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей нашої країни), неухильному захисті національних інтересів України; перманентності заходів з удосконалення законодавства у сфері кібербезпеки; орієнтованості на економічне і соціальне зростання суспільства; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту; визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності; ризик-орієнтованому підході щодо заходів забезпечення кібербезпеки та кіберзахисту; запровадженні механізмів державно-приватного партнерства у сфері кібербезпеки; проактивному підході, що передбачає здійснення випереджувальних заходів; забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

При цьому, у Стратегії закладено інноваційний підхід щодо визначення механізмів її реалізації та критеріїв вимірювання успіхів її практичного впровадження. Очікується, що у перший рік дії нової Стратегії планується невідкладне розроблені індикаторів оцінки стану кібербезпеки і кіберзахисту; огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, запровадження механізмів проведення оглядів стану національної системи кібербезпеки. Це дозволить у перспективі з урахуванням змін у безпековому середовищі вносити зміни до загального плану та щорічних планів заходів з реалізації Стратегії [7].

Проект Стратегії кібербезпеки України розкриває перспективні напрями щодо посилення спроможностей національної системи кібербезпеки. Пріоритетами забезпечення кібербезпеки України визначені: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії.

Головним зовнішньополітичним пріоритетом у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. На цьому фоні, Україна приділятиме особливу увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства, іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти. Для цього наша держава планує розвивати на договірній основі з партнерськими спецслужбами країн-членів ЄС і НАТО взаємовигідний обмін інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використовувати кращі світові практики, активно здійснювати інші спільні заходи, що сприятимуть зміцненню наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки. За таких умов, Україна активно співпрацюватиме з міжнародними партнерами, організаціями та іншими заінтересованими сторонами.

Очікується, що протягом реалізації Стратегії Україна зробить кібербезпеку одним з основних питань своєї міжнародної діяльності, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал держави. З цією метою Україна планує розвивати мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва.

Виходячи із викладеного, та аналізу базових положень проекту Стратегії кібербезпеки України доцільно звернути увагу на те, що, на жаль, поза увагою РНБО України, у рамках визначення планових засад, залишилося питання доцільності підготовки та щорічного оприлюднення на загальнодержавному рівні аналітичного звіту ІОСТА "Оцінка загроз від організованої злочинності в Інтернеті" [8], яка має готуватися на виконання Угоди між правоохоронним агентством ЄС та Україною щодо стратегічного співробітництва [9]. Як переконливо засвідчує європейський досвід, підготовка щорічного звіту ІОСТА є усталеною практикою країн-членів ЄС та залишається важливим інструментом управління та ухвалення політичних рішень, що використовуються фахівцями з протидії кіберзлочинності, у тому числі й транснаціональній, для розробки державних програм на стратегічному рівні, визначення пріоритетів та розподілу ресурсів на операційному рівні.

Підготовка аналітичного звіту ІОСТА мала б велике значення для виконання Угоди між правоохоронним агентством ЄС та Україною щодо стратегічного співробітництва. Також це відповідає Угоді про асоціацію між ЄС та Україною та допомогло б українській владі ефективно впроваджувати у практичну площину базові положення Закону України "Про основні засади забезпечення кібербезпеки в Україні" [10]. Також у документі були б окреслені основні сучасні кіберзагрози та шляхи їх подолання. У подальшому цю аналітичну та статистичну інформацію можна було би використовувати в майбутньому для прийняття стратегічних рішень, розподілу ресурсів та розбудови спроможності на національному рівні. Реагування правоохоронних органів на кіберзлочинність є одним із трьох основних блоків кібербезпеки, поряд із мережевою та інформаційною безпекою та кіберзахистом. На сьогодні в Україні бракує такого комплексного звіту на національному рівні про процеси, пов'язані із кіберзлочинністю, у якому могли б бути окреслені існуючі загрози та вказані рекомендації.

Як слушно зазначає М. Гуцалюк, для посилення боротьби з кіберзлочинністю Європол у 2013 році створив Європейський центр кіберзлочинності (англ. – European Cybercrime Centre, далі – ECC). Починаючи з 2014 року, ECC щорічно готує та оприлюднює Звіт про оцінку загроз організованої кіберзлочинності (англ. – Internet Facilitated Organised Crime Thread Assessment, далі – IOCTA), у положеннях якого досліджуються тенденції та нові загрози, які впливають на уряди, бізнес та громадян ЄС. У цьому звіті значна увага приділяється сферам злочинності, що належать до компетенції ECC, зокрема: кіберзлочини (кібератаки, зловмисне програмне забезпечення, ботмережі та ін.); сексуальна експлуатація дітей в Інтернеті; шахрайство з платіжними картками (викрадення даних карток – "кардінг", "скіммінг"). До інших напрямів, які аналізуються IOCTA, належать так звані наскрізні чинники злочинів, які охоплюють багато сфер злочинності, але самі по собі не завжди є кримінально караними діяннями. Зокрема, це зловживання криптовалютами, відмивання брудних коштів, отриманих злочинним шляхом, компрометація корпоративної електронної пошти тощо [11, с. 121].

За таких умов, завданням оприлюднення звіту IOCTA є інформування політикуму держав, пересічних громадян та представників бізнесу ЄС про здобутки та результати у сфері боротьби з організованою кіберзлочинністю, визначення нових форм та методів кіберзлочинності. Цей звіт має стимулювати відповідальні державні та правоохоронні органи схвалювати рішення на стратегічному, політичному та тактичному рівнях у сфері посилення спроможностей щодо боротьби з кіберзлочинністю та з метою подальшого удосконалення оперативної діяльності правоохоронних органів ЄС.

Висновки.

Саме на Національний координаційний центр кібербезпеки РНБО України покладається обов'язок здійснення та практичної реалізації Стратегії, розробки заходів щодо планування та її виконання, проведення оцінки ефективності впровадження тих чи інших заходів. Щороку Національний координаційний центр кібербезпеки РНБО має оприлюднювати публічний звіт про стан реалізації Стратегії, демонструючи оцінки ефективності проведених заходів. З метою створення умов для проведення оцінки стану забезпечення кібербезпеки необхідно прискорити на державному рівні розробку галузевих індикаторів стану кібербезпеки, що дозволить визначити ефективність реалізації положень Стратегії кібербезпеки.

Таким чином, державне стратегічне планування у сфері забезпечення кібербезпеки передбачає, насамперед, розробку першочергових та позачергових заходів у рамках реалізації положень Стратегії кібербезпеки, визначення організаційно-правового механізму гарантування цифрового суверенітету нашої держави, надійного кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Стратегічне державне планування у сфері забезпечення кібербезпеки має бути спрямоване на: формування та розвиток на державному рівні єдиної науково-технічної політики; вдосконалення нормативно-правової бази з питань кібербезпеки; створення єдиних реєстрів програмних та апаратних комплексів автоматизованої системи управління кібербезпекою; визначення переліку об'єктів критичної інформаційної інфраструктури; створення та функціонування дієвої системи постійного моніторингу кіберпростору; розробку методів та засобів своєчасного виявлення кібератак та кіберзагроз; розробку інформаційних у тому числі й квантових технологій, які дозволять на технологічному рівні покращити стан захисту інформації в інформаційно-телекомунікаційних системах; розробку та створення засобів протидії кіберзброї; розвиток та удосконалення програмно-технічних методів недопущення

витоків, перехоплення або знищення державних інформаційних ресурсів; використання технології нейронних мереж при побудові сучасної архітектури кібербезпеки, які характеризуються коефіцієнтом високої стабільності при пошкодженні своїх структурних елементів тощо.

Державне планування у сфері забезпечення кібербезпеки на виконання положень Стратегії має передбачати розробку щорічного плану заходів та контроль за його виконанням. Потребує вдосконалення система державного стратегічного планування з метою виявлення і запобігання виникненню кризових ситуацій, запровадження нових підходів до оцінки загроз у сфері забезпечення кібербезпеки, забезпечення ефективної координації та функціонування складових державної системи реагування на кібератаки та кіберзагрози. Також при визначенні ефективності національної Стратегії та плану її реалізації слід враховувати показники загального рівня кібербезпеки. Це зокрема, відсоток виконання зобов'язань, рівень прозорості витрат для цілей кібербезпеки (фінансовий аудит конкретних сфер діяльності щодо виконання плану дій з кібербезпеки), результати співробітництва з іншими державами в кіберпросторі тощо.

Також потребує удосконалення державне управління сектором безпеки і оборони, у тому числі системами забезпечення кібербезпеки, захисту інформації та безпеки інформаційних ресурсів; важливим є посилення спроможностей розвідувальних та контррозвідувальних органів шляхом створення організаційних, матеріально-технічних і фінансових умов для концентрації їх оперативних можливостей на пріоритетних напрямах оперативно-службової діяльності, посилення спроможностей суб'єктів забезпечення кібербезпеки для ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, зміцнення інституціональних та технічних можливостей таких суб`єктів, поглиблення міжнародного співробітництва у цій сфері.

Враховуючи викладене, вважаємо за потрібне передбачити у сучасній Стратегії кібербезпеки України на 2021 – 2025 роки положення стосовно доцільності щорічної підготовки загальнонаціонального аналітичного звіту "ІОСТА – Україна", що надасть змогу деталізувати ризики та загрози, здобутки та результати у сфері боротьби з кіберзлочинністю. Таким чином, можна констатувати, що реалізація системних заходів у сфері забезпечення кібербезпеки неможлива без її державного планування як важливої функції державного управління, без прийняття управлінських рішень на планових засадах, що передбачає розробку та вжиття необхідних заходів, визначення алгоритму спільних дій з боку державних органів та інших суб'єктів забезпечення кібербезпеки, встановлення конкретних строків та відповідальних за їх виконання структур, посилення відповідальності виконавців.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

2. Про національну безпеку України: Закон України від 21.06.18 р. № 2469. *Відомості Верховної Ради.* 2018. № 31. Ст. 241.

3. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року "Про організацію планування в секторі безпеки і оборони України": Указ Президента України від 16.05.19 р. № 225/2019. URL: https://zakon.rada.gov.ua/laws/show/225/2019#n2

4. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо

захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.20 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 96/2016.

6. Проект Стратегії кібербезпеки України (2021 – 2025). Безпечний кіберпростір – запорука успішного розвитку України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

7. Робоча група при НКЦК РНБО України схвалила проект Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua/ua/Diialnist/4838.html

8. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

9. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: Закон України від 12.07.17 р. № 2129. URL: https://zakon.rada.gov.ua/laws/show/2129-19#n2

10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

11. Гуцалюк М. Сучасні тенденції організованої кіберзлочинності. *Інформація і право.* № 1(28)/2019. С. 118-128.

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