УДК 004.056.5:343.326 (045)

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Олександра Шаховал, Ірина Лозова, Сергій Гнатюк

Питання кібербезпеки сьогодні гостро постає у всіх державах світу на різних рівнях суспільного життя. У зв'язку із тим, що використання інформаційних ресурсів є необхідністю для нормального функціонування різних галузей народного господарства, потрібно забезпечити захист інформації, яка циркулює в таких системах, на належному рівні. У цій статті викладено дослідження сучасного рівня кібербезпеки в Україні, наведено приклади важливості її забезпечення. Проведено аналіз національних стратегій кібербезпеки держав Європи, Америки, Африки, Азії та Океанії, досліджено термін «кібербезпека» в контексті опрацьованих документів. Висвітлено проблеми сучасного вітчизняного законодавства, що регулює діяльність у сфері кібербезпеки. Також розглянуто причини виникнення перших стратегій кібербезпеки, простежено тенденції у сфері захисту кіберпростору. Відповідно до отриманих результатів запропоновано практичні рекомендації щодо створення національної стратегії кібербезпеки України.

Ключові слова: *національна стратегія, кібербезпека, кібератака, кіберзлочинність, інформаційна безпека, рекомендації.*

Сьогодні спостерігається широке використання сучасних інформаційних та комунікаційних технологій (ІКТ) у державних і недержавних структурах та у суспільстві в цілому. З огляду на виникнення нових загроз та уразливостей, вирішення проблем інформаційної безпеки (ІБ) та кібербезпеки висуваються в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, масова інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Тому, сформована в світі ситуація зобов'язує до побудови загальнодержавної моделі, спрямованої на забезпечення кібербезпеки держави. Через постійне загостренням питання кібербезпеки, вітчизняні та закордонні вчені у своїх роботах [1-9] проводили дослідження базових термінів «кібертероризм», «кібербезпека», «кіберпростір», «кібервплив», «кіберзахист», «кіберзлочин», «кіберінцидент», «кібератака», «кіберінфраструктура» тощо) і намагались дати вичерпні та узагальнюючі дефініції цих понять. У роботі [1] була структурована узагальнена інформація про національні стратегії кібербезпеки різних держав. Проте у нашій державі, на відміну від більшості європейських держав, сьогодні відсутня стратегія забезпечення кібербезпеки – це породжує цілу низку проблем і загроз різного характеру. З огляду на це, *метою* цієї роботи є аналіз ключових положень національних стратегій кібербезпеки різних держав світу для формування рекомендацій щодо розробки вітчизняної стратегії кібербезпеки.

Для досягнення поставленої мети необхідно розв'язати такі задачі: проаналізувати сучасний стан кібербезпеки в Україні та показати важливість створення власної стратегії кібербезпеки; дослідити термін «кібербезпека»; проаналізувати національні стратегії кібербезпеки різних держав; сформулювати практичні рекомендації щодо розробки стратегії кібербезпеки.

Цього року Україна стала абсолютним лідером за кількістю внутрішніх і зовнішніх кіберзагрозами в Європі. За останні роки наша держава неодноразово ставала жертвою не тільки для дрібних шахраїв, але і для широкомасштабних кібероперацій. Експерти Kaspersky Lab сформулювали перелік загроз, які роблять Україну однією з головних «гарячих точок» на кіберкарті світу [10]. Відповідно до цього, можна охарактеризувати ситуацію щодо кібербезпеки в державі таким чином:

1. Однією із причин зараження вірусами програмного забезпечення (ПЗ) українських користувачів є те, що вони використовують неоновлені версії або піратські копії ПЗ.

2. Поширення спамерами спекуляції на темі політичної ситуації в Україні або ж розсилка листів від імені дівчат з України та інших пострадянських держав, які скаржаться на свою нелегку долю і просять перевести кошти на їх рахунки.

3. Україна посідає перші місця у рейтингах світу за ризиками зіткнення з веб-загрозами в третьому кварталі 2015 року. За цей період майже третина українських користувачів мережі зіткнулися із загрозами, що поширюються через Інтернет.

4. Україна має найбільший ризик зараження шкідливими мобільними застосунками. Досить високий для українців і ризик зіткнення з локальними загрозами, до яких відносяться об'єкти, що проникли на комп'ютери шляхом зараження файлів, знімних носіїв або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, ПЗ

в складі складних інсталяторів, зашифровані файли і т.д.).

5. В Україні було зафіксовано велику кількість програм-вимагачів і шифрувальників – шкідливе ПЗ, мета яких – заблокувати пристрій або браузер чи зашифрувати файли користувача, зробивши їх недоступними без спеціального ключа, за який вимагається викуп.

6. Комп'ютери українських чиновників стали жертвами однієї з найскладніших кібершпіонських кампаній Turla. Це угрупування здійснило зараження сотні комп'ютерів більш ніж в 45 державах світу, які є власністю державних установ.

7. Також українці були серед жертв таких кампаній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October.

Правовий фундамент кібербезпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти. Проаналізувавши чинне законодавство, можна стверджувати, що основною проблемою правового забезпечення системи кібербезпеки України є відсутність розробленого та нормативно закріпленого понятійного апарату у сфері кібербезпеки на найвищому рівні. Насамперед, це стратегія забезпечення кібербезпеки, яка стане вітчизняним документом, що врегульовує відносини у кіберсфері та відповідно до якого буде забезпечуватись кібербезпека.

Законодавство щодо кібербезпеки та кіберзлочинності знаходиться на початковій стадії розвитку, а тому українці з їх низьким рівнем обізнаності про загрози використання ІКТ і низьким рівнем ІБ в державі – ідеальні мішені для кіберзлочинців та кібертерористів. У першу чергу, потрібно законодавчо зафіксувати *поняття «кібербезпека»*. Для цього є декілька причин: по-перше, дефініція терміну дозволить визначити предмет досліджень і дискусій, коло проблем, які можуть бути при цьому порушені; по-друге, проблема кібербезпеки через свою специфіку є глобальною і тому найбільш ефективно може бути вирішена тільки за умови об'єднання зусиль широких кіл учасників як на державному рівні, так і на рівні приватних корпорацій та асоціацій. Тому для забезпечення ефективності взаємодії на міжнародному рівні необхідне погодження (стандартизація) розуміння терміну «кібербезпека». Універсального визначення на сьогодні немає, так як кожна держава визначає його по-своєму (інколи такі визначення відрізняються для різних галузей народного господарства). Наведемо деякі з них, які є задекларованими в стратегіях різних держав: 1) бажана ситуація для забезпечення безпеки інформаційних технологій, де ризики глобального кіберпростору будуть знижені до прийнятного мінімуму [11]; 2) бажана ситуація, в якій захист кіберпростору пропорційний кіберзагрозам і можливим наслідкам кібератак [12]; 3) опис захисту ключового правового активу за допомогою конституційних засобів проти технічних, організаційних та природних небезпек, що представляють ризик для безпеки кіберпростору (у тому числі інфраструктури та безпеки даних), а також безпеку користувачів в кіберпросторі [13]; 4) бажаний стан для інформаційного середовища, що дозволяє протидіяти подіям кіберпростору, які можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які там зберігаються, обробляються або передаються. Кібербезпека включає технічну безпеку інформаційного середовища і придатна для боротьби з кіберзлочинністю та створення кіберзахисту [14]; 5) сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, директив, ризик-менеджментових підходів, дій, тренінгів, найкращих практик та технологій, які можуть бути використані для захисту кіберпростору та організацій і користувацьких активів [15].

Сьогодні можна стверджувати, що інформація – це гроші. Особливу увагу варто звертати на інформацію, яка знаходиться в інформаційних системах, онлайн-базах даних, інформаційних ресурсах різних рівнів. Згідно [16] та розуміння необхідності створення умов для забезпечення кібербезпеки і кіберзахисту держави, приведемо ситуації в закордонних установах, які не були готові до хакерських атак, внаслідок чого понесли великі втрати даних, а, отже, і матеріальні: Scottrade – викрадено детальну інформацію про 4,6 млн клієнтів; Excellus BlueCross BlueShield – витік більш ніж 10 млн записів, які включали в себе імена, дати народження, номери соціального страхування і поштові адреси, а також деякі фінансові рахунки; Carphone Warehouse – викрадено особисті дані близько 2,4 млн клієнтів (4% населення), а також їх зашифровані дані кредитних карток; аптечна мережа CVS – втрата даних кредитних карток, адрес електронної пошти та поштових адрес, номерів телефонів і паролів невідомої кількості клієнтів; UCLA Health – втрата 4,5 млн записів, які

включають номери соціального страхування, і навіть медичних даних клієнтів; U.S Office of Personnel Management – отримано доступ до конфіденційної інформації; Anthem – страхова компанія втратила більше 80 мільйонів записів про клієнтів від номерів соціального страхування до конфіденційної інформації; Donald Trump's hotel – крадіжка даних кредитних карт (в тому числі коди і номери карт) в готелях фірми по всій території США.

Перші стратегії кібербезпеки з'явились на початку минулого десятиріччя [1]. Однією з перших держав, що сприйняла кібербезпеку як питання державного рівня, була США, де 2003 року було опубліковано Національну стратегію безпеки в кіберпросторі. У наступні роки в Європі поширювались плани заходів та стратегії, покликані розв'язати подібну задачу. Через велику кібератаку 2007 року Естонія стала однією з перших держав-членів Євросоюзу, яка опублікувала 2008 року національну стратегію кібербезпеки, у якій особливу увагу зосереджено на безпеці ІКТ.

У зв'язку із тим, що вітчизняна стратегія кібербезпеки досі не затверджена, а лише прийнято проект за основу, варто детально розглянути і звернути увагу на ключові аспекти стратегій держав, які працюють у цьому напрямку не перший рік. Розглянемо деякі з них:

І. Держави Європи. Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) 2011 року [17] створена з метою кримінального переслідування кібератак та запобігання їх виникнення, а також запобігання виходу з ладу ІТ-обладнання через випадкові чинники. Передбачено такі загрози: кібератаки та виведення з ладу критичних інформаційних ресурсів. До принципів забезпечення кібербезпеки віднесено узгодження набору інструментів для реагування на кібератаки; регулярна оцінка ситуації, ризиків та прийняття відповідних засобів захисту; регулярні тренування персоналу та тестування обладнання; зміцнення ІТ-безпеки в сфері держуправління. Наведено дефініції таких понять як кіберпростір, кібератака, кібершпіонаж, кіберсаботаж, кібербезпека, цивільна та військова кібербезпека, критична інфраструктура (критичні ресурси). Міжнародна співпраця і партнерство, регулярна перевірка мети стратегії на рівень її досягнення та оновлення відповідно до стану поточної ситуації є пріоритетними.

Стратегія кібербезпеки Угорщини (National Cyber Security Strategy of Hungary) [18], що була прийнята 2013 року, спрямована на розвиток вільного та безпечного кіберпростору і захист національного суверенітету в національному та міжнародному контексті, який зазнав значних змін у зв'язку із появою кіберпростору, що став новим ключовим чинником у XXI сторіччі. Крім того, вона спрямована на захист діяльності та забезпечення безпеки національної економіки і суспільства, адаптації технологічних інновацій для полегшення економічного зростання і міжнародного співробітництва в цій галузі відповідно до національних інтересів Угорщини. Дефініцій понять у документі не наведено. Пріоритетними є співпраця на різних рівнях, підвищення рівня обізнаності та освіченості громадян в сфері кібербезпеки, захист дітей у кіберпросторі, розвиток нормативно-правової та технічної бази, мотивація комерційного сектору.

Стратегія кібербезпеки Чорногорії (Strategy on Cyber Security of Montenegro to 2017) [19] була прийнята 2013 року. Мета документу – побудувати інтегрований, функціональний та ефективний кіберпростір, відповідно до міжнародних стандартів і принципів. У документі наведено дефініції таких понять: кіберпростір, ІБ, комп'ютерна безпека, Інтернет-безпека, мережева безпека, кібербезпека, кібероборона, кіберзлочин, кібертероризм, кібершпіонаж, кібервійна. Визначено такі загрози: DoS і DDoS-атака, атаки на сайти з метою несанкціонованої модифікації їх змісту, несанкціонований доступ до розвинутих ІКТ державних органів та їх бази даних, фішинг. До принципів забезпечення кібербезпеки віднесено визначення інституційної та організаційної структури в сфері кібербезпеки в державі, захист критичних інформаційних структур, зміцнення потенціалу державних правоохоронних органів, реагування на інциденти, посилення ролі Міністерства оборони та військових Чорногорії в кіберпросторі, державно-приватне партнерство, підвищення обізнаності громадськості та захисту користувачів. Пріоритетними визначено такі завдання: моніторинг ризиків на національному рівні, розробка чіткої структури управління, створення механізмів розслідування інцидентів, встановлення балансу між безпекою і повагою приватного життя, створення конфіденційних механізмів обміну інформацією, встановлення основних вимог до кібербезпеки, відповідальність за кіберзлочинність, зміцнення програм освіти і професійної підготовки, підвищення обізнаності громадськості з питань кібербезпеки тощо.

Метою Стратегії кібербезпеки Естонії (Cyber Security Strategy) [11] 2014 року є опис методів забезпечення безперебійної експлуатації та стійкості

важливих сервісів і захист критичних інформаційних інфраструктур від кіберзагроз на період до 2017 року. У документі наведено дефініцію поняття кібербезпека. Головним пріоритетом у забезпеченні кібербезпеки є прогноз як запобігання можливості виникнення загрози, так і ефективного реагування на загрози, які матеріалізуються. Визначено такі загрози: кібератаки, шпіонаж, кіберзлочини. Принципи забезпечення кібербезпеки: кібербезпека є невід'ємною частиною національної безпеки, підтримує функціонування держави і суспільства, конкурентоспроможність економіки та інновацій, забезпечується на основі принципу пропорційності, беручи до уваги існуючі та потенційні ризики і ресурси; гарантується дотриманням основних прав і свобод, а також захисту особистої інформації та особистості; починається з індивідуальної відповідальності за безпечне використання засобів ІКТ; підтримується інтенсивністю і конкурентоспроможністю досліджень і розвитку на міжнародному рівні; забезпечується на узгодженій основі в рамках співпраці між державним, приватним та третім сектором, беручи до уваги взаємозв'язок і взаємозалежність існуючої інфраструктури і сервісів в кіберпросторі; забезпечується за допомогою міжнародного співробітництва з союзниками і партнерами. Завдяки співпраці, Естонія сприяє зміцненню глобальної кібербезпеки і підвищує рівень своєї компетенції.

Стратегія кібербезпеки Австрії (Austrian Cyber Security Strategy) 2013 року [13] має на меті визначення ролей, обов'язків та повноваженнь державних і недержавних суб'єктів у кіберпросторі, а також створення адекватних структурованих умов для співпраці між усіма суб'єктами. Визначено такі загрози: маніпулювання у каналах зв'язку; маніпулювання в системах фінансових операцій; DDoS-атаки; відсутність правової основи; відсутність безпеки, обізнаності та стандартів; систематична крадіжка цифрових персональних даних; махінації в соцмережах; недостатня кількість експертів; виробничий кібершпіонаж, відсутність систематичного оцінювання технологічного впливу; шкідливе ПЗ, проблемні і несумісні коди ПЗ; непевна відповідальність в урядових системах, потреба в стратегії мережевої інфраструктури. До принципів забезпечення кібербезпеки віднесено наступне: дотримання закону, самоврегулювання, пропорційність, ієрархічність, конфіденційність, цілісність, автентичність, доступність, приватність і захист даних. Стратегією передбачено такі пріоритети покращення стійкості критичних інфраструктур: посилення культури кібербезпеки; зміцнення досліджень Австрії в сфері кібербезпеки; ефективна співпраця з Європою та світом у сфері кібербезпеки.

Стратегія кібербезпеки Польщі (Cyberspace Protection Policy of the Republic of Poland) [20] була ухвалена 2013 року. Відповідно до документу, інфраструктура ІКТ повинна бути захищена від атак з кіберпростору, знищення, пошкодження та несанкціонованого доступу. Наведено дефініції таких понять: експлуатація з порушенням норм, кіберпростір, кіберзлочин, безпека кіберпростору, кібератака, кібертероризм, CERT, кіберпростір Республіки Польща, користувач кіберпростору, інцидент комп'ютерної безпеки, ризик-менеджмент тощо. Принципи забезпечення кібербезпеки, дотримання яких є пріоритетними: принцип законодавчих заходів, принцип процедурних і організаційних заходів (система менеджменту), принцип виховання, навчання та підвищення обізнаності в галузі безпеки, принцип технічних дій (збільшення кількості команд для реагування на інциденти безпеки у державних установах, тестування рівня безпеки, розвиток системи попередження, запобігання інцидентам і прийняття профілактичних рішень) [10].

ІІ. Держави Африки. Стратегія кібербезпеки Кенії (Cybersecurity Strategy) [21] була затверджена 2014 року. Метою є чітке визначення бачення кібербезпеки Кенії, цілі та завдання для забезпечення захисту кіберпростору держави, продовжуючи сприянню використання для економічного зростання Кенії. Визначено такі загрози: ботнети, організована злочинність, DoS-атаки, кібертероризм, шкідливі коди та спеціально націлене шкідливе ПЗ. У стратегії наведено дефініції понять CERT, кіберпростір, кібербезпека, електронне урядування, критична інфраструктура, уряд, ІКТ, інсайдерська загроза, соціальний інжиніринг тощо. Пріоритетними напрямками визначено електронне урядування, підвищення кібербезпеки Кенії, оновлення стратегії, її цілей і завдань.

Стратегія кібербезпеки Маврикія (National Cyber Security Strategy 2014-2019) [22] була затверджена 2014 року. Метою документу є інтеграція ІБ в базові структури для розвитку інформаційного суспільства. Підхід до виконання стратегії базується на задачах кібербезпеки: побудова безпеки за функціональними і технічними вимогами, робота системи моніторингу кіберзагроз, яка сприяє кращому реагуванню, моніторингу та координації кіберзагроз на національному рівні у режимі 24/7, покращення ризик-менеджменту, покращення і замовлення експертиз та їх супровід. Дефініцій

понять і загроз у стратегії не наведено. Пріоритетними є вибір правильного фокусу для створення безпечного комп'ютеризованого середовища, оприлюднення механізму для видалення нелегального контенту, посилення правоохоронної спроможності в кібербезпеці, міжнародна і регіональна співпраця, посилення безпеки в кіберпросторі, створення тестувальної системи для мережі безпеки, сприяння розробці ПЗ, сприяння виконанню стандартів ІБ в цивільних справах, проведення аудитів, співробітництво з промисловістю для пошуку покращень, створення тренінгових програм, покращення кіберосвіти та обізнаності людей у цій сфері, організація щорічних заходів, присвячених міжнародній кібербезпеці.

III. Держави Азії та Океанії. Стратегія кібербезпеки Катару (Qatar's National Cyber Security Strategy) [23] була прийнята 2014 року та являє собою план для поліпшення ІБ держави. Метою документу є встановлення і підтримка безпечного кіберпростору для захисту національних інтересів і збереження основних прав та цінностей суспільства Катару. У документі визначено такі загрози: інсайдерські атаки, хактивізм, кібератаки, кіберзлочини, APT-загрози. Наведено дефініції понять: інформаційна кампанія, функціональні можливості, критична інформаційна інфраструктура, кіберзлочин, критичний сектор, організація критичного сектору, кібербезпека, контроль кібербезпеки, кіберпростір, персональна інформація, здатність до відновлення нормального функціонування, ненавмисні інсайдери. Стратегією визначено наступні принципи забезпечення кібербезпеки: катарський уряд несе відповідальність за захист своєї інформації, систем і мереж; інвестиції в людські ресурси, процеси і технології, необхідні для забезпечення функціонування сервісів, на які опирається суспільство; визначення напрямку для подальшого економічного розвитку Катару; можливість підприємств захищати свою інформацію і мережі від кіберзагроз, впровадження передового досвіду. До пріоритетів віднесено наступне: мінімізація ризиків, сприяння встановленню високого рівня кібербезпеки в Катарі, забезпечуючи стратегічний напрямок для зусиль в області кібербезпеки, і тісна співпраця із організаціями для повного виконання цілей і вимог стратегії, чітке дотримання плану дій тощо.

Концепція кібербезпеки Сінгапуру (National Cyber Security Masterplan 2018) [24] затверджено 2013 року. Вона спрямована на створення безпечного і стійкого середовища інфокомунікацій та динамічної екосистеми кібербезпеки. Документом передбачено такі загрози: APT-загрози, фішинг, соціальний інжиніринг, DDoS-атаки, шкідливе ПЗ. Дефініцій понять у концепції не наведено. Пріоритетом є підвищення рівня готовності та реагування на значні кібератаки на національному рівні, оцінка безпеки ІКТ, які мають вирішальне значення для функціонування критичних інфраструктур, збільшення людських та інтелектуальних ресурсів тощо.

Стратегія кібербезпеки Бангладешу (The National Cybersecurity Strategy of Bangladesh) [25] була прийнята 2014 року. Метою документу є створення цілісного уявлення про Бангладеш як про безпечну та процвітаючу державу у координації уряду, приватного сектору, громадян та міжнародних зусиль в обороні кіберпростору до 2021 року. У документі визначено такі принципи забезпечення кібербезпеки: дослідження атак; внутрішня і зовнішня співпраця; створення законів, які взаємодіють між собою і застосовуються глобально; створення організацій кібербезпеки; тренування навиків персоналу; визначення правової та оперативної основи для комплексної та повної координації державного партнерства з приватним сектором у сфері кібербезпеки; захист урядової інфраструктури; можливість вчасного реагування на інциденти ІБ. Дефініцій понять у документі не наведено. Крім того, визначено загрози від шпіонажу до фішингу, DoS-атаки, інші кіберзлочини. Визначено такі пріоритети держави: покращення законодавства; технічні і процедурні заходи (організаційні структури і політика кіберзлочинності, спостереження, оповіщення і реагування на інциденти, а також створення загальної та універсальної цифрової системи ідентифікації); організаційні структури (фокус на національні межі протоколів безпеки, стандартів і схем акредитації ПЗ).

Концепція кібербезпеки Індії (National Cyber Security Policy) [26] була затверджена 2013 року. Метою документу є побудова захищеного і стійкого кіберпростору, захист інформації та інформаційної інфраструктури в кіберпросторі, створення можливості для реагування і запобігання кіберзагрозам, зменшення уразливостей і мінімізація шкоди від кіберінцидентів. Завдання кібербезпеки, які є пріоритетними для Індії – створення безпечної кіберекосистеми; створення системи ресурсів; заохочення відкритих стандартів; збільшення можливостей регулюючих структур; створення механізмів захисту від нових загроз, управління уразливостями реагування на загрози безпеці; захист електронних урядових сервісів; захист

і стійкість критичної інформаційної інфраструктури; розвиток людських ресурсів; поширення інформації та співпраця тощо.

IV. Держави Америки. Стратегія кібербезпеки США (International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World) [27] 2011 року визначає контекст підходу для розуміння пріоритетів держави, способів досягнення її безпечного кіберпростору та боротьби з кібератаками. У якості загроз визначено шантаж та вимагання коштів, шахрайство, крадіжки та експлуатація дітей, крадіжка інтелектуальної власності. Дефініцій понять у документі не наведено. Забезпечення кібербезпеки держави базується на таких принципах: дотримання основних свобод; приватність особистого життя; вільний потік інформації; повага до різних форм власності; захист від злочинів; відповідна законодавча база; взаємодія на глобальному рівні; багатостороннє управління. Пріоритетами США у цій сфері є захист інтелектуальної власності, у тому числі комерційних таємниць; взаємодія та відповідність технічних стандартів, встановлених експертами; сприяння співробітництву та партнерству; управління інцидентами, стійкість і можливості відновлення інформаційної інфраструктури; проведення консультацій з промисловим сектором; участь у розробці міжнародних стандартів; фокусування законів про кіберзлочинність на боротьбі з незаконною діяльністю; створення і розширення вже існуючих військових союзів для протистояння потенційним загрозам в кіберпросторі; заохочення міжнародного співробітництва для ефективного комерційного захисту конфіденційних даних.

Концепція кібербезпеки Канади (Action Plan 2010-2015 for Canada's Cyber Security Strategy) [28] 2013 року призначена для спрямування зусиль уряду для створення безпечного кіберпростору для канадців. У документі визначено такі принципи забезпечення кібербезпеки: захист державних систем; співпраця з метою захисту ключових систем від кібератак, що знаходяться за межами федерального уряду; забезпечення безпеки канадців в онлайн-мережі. У якості загроз визначено різного роду кіберзлочини та кібератаки. Дефініцій понять не наведено. Пріоритетними визначено наступні дії: безпечне зберігання особистої інформації канадців онлайн, а також ІКТ, інфраструктури уряду; боротьба з кіберзлочинністю; посилення безпеки кіберсистем федерального рівня та підвищення інформованості суспільства в галузі кібербезпеки.

Стратегія кібербезпеки Ямайки (Jamaica National Cyber Security Strategy) [29] була прийнята 2015 року. Мета документу – взяти до уваги забезпечення ведення онлайн та оффлайн справ. Визначено такі загрози: викрадення персональних даних; фішинг; підроблені банківські застосунки; атаки на комп'ютерні дані та системи; поширення дитячого сексуального насильства; шахрайські Інтернет-аукціони, віруси, ботнети, внутрішні загрози тощо. Наведено дефініції понять: ботнет, критична інфраструктура, кіберзлочин, кібербезпека, ІБ, CERT, відмова в обслуговуванні, фішинг, саморегулювання, несанкціонований доступ, несанкціонована зміна. Пріоритети держави у цій сфері – інформованість населення в сфері кібербезпеки; розвиток культури кібербезпеки; захист національної критичної інфраструктури; тренінги для громадськості тощо.

Отже, проаналізувавши стратегії та з огляду на постійне збільшення ризику виникнення нових кіберзагроз та їх еволюції, збільшення впливу на особу, суспільство, кожній державі необхідно мати продуману та чітко сформульовану, комплексну стратегію кібербезпеки. Оскільки загрози такого типу не мають кордонів, потрібно постійно підтримувати тісне міжнародне співробітництво, що є необхідним не лише для підготовки до кібератак, а й для своєчасного реагування на них. Провівши аналіз ключових положень національних стратегій кібербезпеки держав світу та врахувавши сучасний стан цієї галузі в Україні, при розробці вітчизняної стратегії кібербезпеки необхідно:

1) розробити *єдиний понятійний апарат,* у якому чітко визначити терміни й поняття, пов'язані із забезпеченням кібербезпеки держави (вони мають бути узгодженими з міжнародними стандартами і враховувати національні особливості);

2) визначити *основні загрози та критичні інфраструктури держави,* забезпечення кібербезпеки яких є найбільшим пріоритетними (розробити механізми ідентифікації та пріоритезації найбільш важливих об'єктів інформаційної інфраструктури);

3) визначити *основні принципи забезпечення кібербезпеки* держави та усіх її стейкхолдерів (врахувати усі їх інтереси в різних сферах, а також питання взаємовпливу та співпраці);

4) створити *систему державних органів,* на які покладаються завдання щодо забезпечення кібербезпеки, чітко визначити їх обов'язки та межі відповідальності;

5) приділити увагу *багаторівневій системі підготовки фахівців* у сфері кібербезпеки (передбачити різні освітні напрямки для фахівців, орієнтованих на різні галузі народного господарства);

6) врахувати *зміни у суміжних нормативно-правових актах* шляхом внесення поправок чи прийняття нових їх редакцій (зокрема це стосується тих документів, які на сьогодні становлять правовий фундамент забезпечення кібербезпеки нашої держави);

7) передбачити усі види *відповідальності за різного роду правопорушення та злочинів* у кіберпросторі;

8) визначити *часові рамки* реалізації стратегії, *відповідальні* за кожен напрямок підрозділи, передбачити можливість *адаптації* стратегії відповідно до міжнародних норм та актуальних викликів у кіберпросторі, а також *проведення зовнішнього аудиту* виконання передбачених у стратегії заходів.

ЛІТЕРАТУРА

[1]. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. – Том 19. – №2. – 2013. – С. 118-129.

[2]. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов // Правова інформатика. – №2(42). – 2014. – С. 54-62.

[3]. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д.В. Дубов. – К.: НІСД, 2014. – 328 с.

[4]. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К. : НАУ. – 2013. – 432 с

[5]. Словник термінів з кібербезпеки / За заг. ред. Копана О.В., Скулиша Є.Д. – К.: ВБ «Аванпост-Прим». – 2012. – 214 с.

[6]. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф., 22 березня 2011. – К.: Вид-во НА СБ України, 2011. – Ч.2. – С. 43-48.

[7]. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі / В.О.Гнатюк //Безпека інформації. – Том 19, №3. – 2013. – С.175-180.

[8]. Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр.: Вип. 4 (28). – К. : НАУ, 2009. – С. 131-140.

[9]. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти // О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк / Безпека інформації. – Том 19, №1. – 2013. – С. 40-45.

[10]. 8 тезисов про кибербезопасность в Украине. [Електронний ресурс]. – Режим доступу: http://ain.ua/2015/11/25/617473

[11]. Cyber Security Strategy of Estonia [Електронний ресурс]./ Ministry of Economic Affairs and Communication. – 2014. – Режим доступу: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[12]. Cyber Security Strategy for Defence of Belgium [Електронний ресурс]./ Strategy Department. – 2014. – Режим доступу: https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf

[13]. Austrian Cyber Security Strategy [Електронний ресурс]. – Vienna, 2013. – Режим доступу: https://www.bka.gv.at/DocView.axd?CobId=50999

[14]. Défense et sécurité des systèmes d'information Stratégie de la France [Електронний ресурс]/Agence Nationale de la Sécurité des Systèmes d'information. – 2011. – Режим доступу: https://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

[15]. Latvian cyber security strategy for the period 2014 to 2018 [Електронний ресурс]. – 2014. – Режим доступу: https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf

[16]. These companies lost your data in 2015's biggest hacks, breaches [Електронний ресурс]. – 2015. – Режим доступу: http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2015/

[17]. Cyber Security Strategy for Germany [Електронний ресурс]./ Federal Ministry of the Interior. – Berlin, 2011. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

[18]. National Cyber Security Strategy of Hungary [Електронний ресурс]./ Prime Minister's Office. – Budapest, 2013. – Режим доступу: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf

[19]. Strategy on Cyber Security of Montenegro to 2017 [Електронний ресурс]. – Podgorica, 2013. – Режим доступу: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies- ncsss/CyberSecurityStrategyforMontenegro.pdf

[20]. Cyberspace Protection Policy of the Republic of Poland [Електронний ресурс]./ Ministry of Administration and Digitisation, Internal Security Agency. – Warsaw, 2013. – Режим доступу: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf

[21]. Cybersecurity Strategy [Електронний ресурс]./ Ministry of Information Communications and Technology. – Nairobi, 2014. – Режим доступу: http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf

[22]. National Cyber Security Strategy 2014-2019 [Електронний ресурс]. – 2014. – Режим доступу: http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf

[23]. Qatar National Cyber Security Strategy [Електронний ресурс]./ Department of Comunications, Energy & Natural Resourses. – 2015. – Режим доступу:

http://docplayer.net/2856349-National-cyber-security-strategy-2015-2017.html
[24]. National Cyber Security Masterplan 2018. [Електронний ресурс]./ Infocomm Development Authority of Singapore. – 2013. – Режим доступу: https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf
[25]. National Cybersecurity Strategy [Електронний ресурс]. – 2014. – Режим доступу: http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf
[26]. National Cyber Security Policy [Електронний ресурс]./ Ministry of Comunication and Information Technology, Department of Electronics and Information Technology. – New Delphi, 2013. – Режим доступу: http://deity.gov.in/content/national-cyber-security-policy-2013-1
[27]. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World [Електронний ресурс]. – Washington, 2011. Режим доступу: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[28]. Action Plan 2010-2015 for Canada's Cyber Security Strategy [Електронний ресурс]./ Government of Canada's. – 2013. – Режим доступу: http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf
[29]. Jamaica National Cyber Security Strategy [Електронний ресурс]./ Government of Jamaica. – 2015. – Режим доступу: http://mstem.gov.jm/sites/default/files/Jamaica%20National%20Cyber%20Security%20Strategy.pdf

REFERENCES

[1]. Gnatyuk S. Cyberterrorism: development history, current trends & countermeasures, 2013, Ukrainian Scientific Journal of Information Security, №19(2), p. 118-129.
[2]. Baranov O.A. About the interpretation and definition of «cybersecurity», Pravova informatika, №2(42), 2014, p.54-62.
[3]. Dubov D. Cyberterrorism as a new dimension of geopolitical rivalry: monograph. 2014, K.: NISD, 328 p.
[4]. Buryachok V. Guidelines for the development of the cyber security state system: monograph, 2013, K.: NAU, 432 p.
[5]. Slovnyk terminiv z kiberbezpeky / Za zag. red. Kopana O.V., Skulysha E.D., K.: VB Avanpost-Prym, 2012, 214 p.
[6]. Melnyk V., Nyhomyrov O. Do problem formuvannya ponyatiyno-terminologichnogo aparatu kiberbezpeky // Actualni problem upravlinnya informatsiynoyu bezpecou derzhavy: zb. nauk. pr. conf., 22.03.2011, P. 43-48.
[7]. Gnatyuk V. Analysis of «incident» definitions and its interpretation in cyberspace // Ukrainian Scientific Journal of Information Security, №19(3), 2013, P.175-180.
[8]. Harchenko V.P. Kiberterrorizm na aviatsionnom transporte // Problemi informatizatsiyi ta upravlinnya: zb. nauk. pr., K.: NAU, 2009, P.131-140.
[9]. Korchenko O., Buryachok V., Gnatyuk S. Cybernetic security of the state: characteristic features & problem aspects // Ukrainian Scientific Journal of Information Security, №19(1), 2013, p. 40-45.
[10]. 8 tezysov o kyberbezopasnosti v Ukraine [Electronic resourse]. – Access mode: http://ain.ua/2015/11/25/617473
[11]. Cyber Security Strategy of Estonia, 2014 [Electronic resourse]. –Access mode: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014 - 2017_public_version.pdf
[12]. Cybersecurity Strategy for Defence of Belgium, 2014. [Electronic resourse]. – Access mode: https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf
[13]. Austrian Cyber Security Strategy, 2013, Vienna [Electronic resourse]. – Access mode: https://www.bka.gv.at/DocView.axd?CobId=50999
[14]. Défense et sécurité des systèmes d'information Stratégie de la France, 2011 [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011
[15]. Latvian cyber security strategy for the period 2014 to 2018, 2014 [Electronic resourse]. – Access mode: https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf
[16]. These companies lost your data in 2015's biggest hacks, breaches, 2015 [Electronic resourse]. – Access mode: http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2015/
[17]. Cyber Security Strategy for Germany, 2011, Berlin [Electronic resourse]. – Access mode: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
[18]. National Cyber Security Strategy of Hungary, 2013, Budapest [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf
[19]. Strategy on Cyber Security of Montenegro to 2017, 2013, Podgorica [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CyberSecurityStrategyforMontenegro.pdf
[20]. Cyberspace Protection Policy of the Republic of Poland, 2013, Warsaw [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf
[21]. Cybersecurity Strategy, 2014, Nairobi [Electronic resourse]. – Access mode: http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf
[22]. National Cyber Security Strategy 2014-2019, 2014 [Electronic resourse]. – Access mode: http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf
[23]. Qatar National Cyber Security Strategy, 2015 [Electronic resourse]. – Access mode: http://docplayer.net/

2856349-National-cyber-security-strategy-2015-2017.html
[24]. National Cyber Security Masterplan 2018, 2013 [Electronic resourse]. – Access mode: https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf
[25]. National Cybersecurity Strategy, 2014 [Electronic resourse]. – Access mode: http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf
[26]. National Cyber Security Policy, 2013, New Delphi [Electronic resourse]. – Access mode: http://deity.gov.in/content/national-cyber-security-policy-2013-1
[27]. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, 2011, Washington [Electronic resourse]. – Access mode: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[28]. Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013 [Electronic resourse]. – Access mode: http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf
[29]. Jamaica National Cyber Security Strategy, 2015 [Electronic resourse]. – Access mode: http://mstem.gov.jm/sites/default/files/Jamaica%20National%20Cyber%20Security%20Strategy.pdf

РЕКОМЕНДАЦИИ ПО РАЗРАБОТКЕ СТРАТЕГИИ КИБЕРБЕЗОВАСНОСТИ УКРАИНЫ

Проблема кибербезопасности сегодня достаточно остро постает во всех государствах мира на разных уровнях общественной жизни. В связи с тем, что использование информационных ресурсов является необходимостью для нормального функционирования различных отраслей народного хозяйства, нужно обеспечить защиту информации, которая циркулирует в таких системах, на должном уровне. В данной статье изложено исследование уровня кибербезопасности в Украине и приведены примеры важности ее обеспечения. Проведено анализ национальных стратегий кибербезопасности различных государств Европы, Америки, Африки, Азии и Океании, исследован термин «кибербезопасность» в контексте обработанных документов. Освещено проблемы современного отечественного законодательства, регулирующего деятельность в сфере кибербезопасности. Также рассмотрены причины появлений первых стратегий кибербезопасности, прослежены тенденции в сфере защиты киберпространства. Согласно полученным результатам, предложены практические рекомендации по созданию национальной стратегии кибербезопасности Украины.

Ключевые слова: национальная стратегия, кибербезопасность, кибератака, киберпреступность, информационная безопасность, рекомендации.

RECOMMENDATIONS FOR CYBERSECURITY STRATEGY OF UKRAINE DEVELOPMENT

The problem of cybersecurity is quite acuted in all states of the world in different levels of social life. Using of informational resources is necessary for normal functioning of various sectors of the economy. It is important to secure information that circulates in such systems, at the appropriate level. The research of level of cybersecurity in Ukraine and examples of its importance are presented in this paper. The analysis of cyber security strategies of the various states of Europe, America, Africa, Asia and Oceania, investigated the term «cybersecurity» from the context of these documents were done. The problems of modern national legislation regulating the activities in the sphere of cybersecurity were highlighted. Also the causes of the first cyber security strategy was studied, and also modern trends in the cyberspace security were analyzed. According to the results, practical recommendations for creating the national cyber security strategy of Ukraine were proposed.

Index terms: national strategy, cybersecurity, cybercrime, cyberterrorism, information security, recommendations.

Шаховал Олександра Анатоліївна, студентка кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: alexandra.shakhoval@yandex.ru
Шаховал Александра Анатольевна, студентка кафедры безопасности информационных технологий Национального авиационного университета.
Shakhoval Alexandra, Student of IT-security Academic Dept in National Aviation University.

Лозова Ірина Леонідівна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: kira1983@yandex.ua
Лозовая Ирина Леонидовна, старший преподаватель кафедры безопасности информационных технологий Национального авиационного университета.
Lozova Iryna, Senior Lecturer of IT-security Academic Dept in National Aviation University.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua
Гнатюк Сергей Александрович, кандитат технических наук, доцент, доцент кафедры информационных технологий Национального авиационного университета.
Gnatyuk Sergiy, PhD in Eng, Associate Professor of IT-security Academic Dept in National Aviation University.