Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Категорія «Б», Наказ Міністерства освіти і науки України від 28.12.2019 №1643)
www.dy.nayka.com.ua | № 3 2020 р. | 26.03.2020

DOI: 10.32702/2307-2156-2020.3.30

УДК 351.865

Є. В. Котух,
к. т. н, доцент кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів, м. Дніпро
ORCID: 0000-0003-4997-620X

ФОРМУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ

Ye. Kotukh
PhD in Technical Sciences,
Associate Professor of Cyber Security and Information Technologies Department,
University of Customs Service and Finances, Dnipro

FORMATION OF CYBER SECURITY SYSTEMS IN PUBLIC AUTHORITIES

Сучасна організаційна перебудова державної влади в Україні створює відповідні виклики для самої країни, бізнесу та окремо взятої фізичної особи, особливо це стосується питання захисту у кіберпросторі. Доведено, що ефективні системи кібербезпеки здатні захистити різноманітні комунікації та посилити довіру до влади. Найбільший успіх в цьому питанні може бути досягнутий за умов співпраці різних зацікавлених акторів у кіберпросторі, що посилить їх позитивну взаємозалежність. На основі аналізу загальних принципів та основних особливостей систем кібербезпеки визначено чотири аспекти їх унікальності: 1) заохочувані дії; 2) драйвери; 3) середовище та 4) аудиторія. Запропоновано поділити основні поняття кібербезпеки на дві групи відповідно до їх змісту: 1) виміри кібербезпеки; 2) дії, необхідні для забезпечення кібербезпеки в органах публічної влади. Сформульовано перелік дій, необхідних для забезпечення кібербезпеки в органах публічної влади.

The modern organizational restructuring of public administration system in Ukraine poses challenges for the country, business and individuals, and especially as regards the issue of protection in cyberspace. Effective cybersecurity approaches can protect a large number of communications and build trust to government. The greatest success in this issue can be achieved through the cooperation of various stakeholders in cyberspace, which will enhance their positive interdependence. Based on an analysis of the general principles and key features of existing cyber security systems, four aspects of their uniqueness have been identified: 1) encouraged actions; 2) drivers; 3) the environment and 4) the audience. Encouraged action is a desirable or recommended action related to the main content of the cyber security system; driver is the factor that motivated its creation; environment is a situation in which you can use the system; audience - likely users of cybersecurity. Focus is on five dimensions of cybersecurity: human, organizational, infrastructure, technological and regulatory.
Five cybersecurity issues that are most commonly discussed in cybersecurity systems are also considered: human, organization, infrastructure, technology (legislation) and regulation.

Implementing a cyber security project in public administration is not easy, it involves continuous improvement, monitoring, analysis and diagnostics, taking into account the life cycle of the cybersecurity system.
It is proposed to divide the basic concepts of cybersecurity into two groups according to their content: 1) dimensions of cybersecurity; 2) actions required to ensure cyber security in public authorities. The list of actions that should be taken into account when developing appropriate information systems to ensure cybersecurity in public authorities was formulated. These include: building trust on the Internet; coordination, cooperation and collaboration; profiling of cybernetic state; facilitating the implementation of cybersecurity systems; review and evaluation; creating a legal environment and appropriate standards.

Ключові слова: *система кібербезпеки; кіберстратегія; кіберспроможність; забезпечення кібербезпеки; публічна влада.*

Keywords: *cybersecurity system; cyber-strategy; cyber-ability; cyber security providing; public power.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В сучасних умовах все більше підприємств, незалежно від того, чи вони належать до сфери виробництва або надання послуг, все більше спираються на інформаційні технології. Навіть якщо це не так глобально, то під час ведення бізнесу, зважаючи на тенденцію діджиталізації, вони створюють комунікації зі стейкхолдерами у інформаційному просторі. Ефективні системи кібербезпеки здатні забезпечити захист таких комунікацій та посилити довіру до влади. Зважаючи на це актуальним напрямком наукових досліджень останнім часом залишається аналіз сучасних тенденцій та пріоритетних заходів із забезпечення кібербезпеки в публічному секторі.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Тенденції розвитку публічного управління досліджено у наукових працях Т. Бєльської, В. Гриневич, В. Дзюндзюка, В. Єлагіна, Д. Карамишева та ін. Питанням створення систем кібербезпеки у механізмі національної безпеки присвячено наукові праці І. Діордіци, Є. Живила, З. Коваля, В. Куцаєва, В. Ліпкана, С. Срібного, В. Ткаченка, В. Шеломенцева та ін. Серед іноземних праць хотілося б окремо виділити напрацювання Р. Азмі, К. Андреассона, Е. Камарка, П. Кеніса, К. Прована та ін. Проте в сучасних умовах глобалізації виникають нові умови та проблемні питання, які вимагають зміни підходів щодо визначення особливостей кіберзагроз, формування відповідної культури кібербезпеки в органах публічного управління, організації її забезпечення.

Формулювання цілей статті (постановка завдання). В статті за мету обрано обґрунтування організаційних проблем та напрямків формування систем кібербезпеки в органах публічної влади.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Активна розробка та впровадження систем кібербезпеки (СКБ) на різних рівнях почались з початку 2000-х років. При цьому загальні принципи та основні особливості таких систем кібербезпеки знайшли відображення у низці керівних документів, основні з яких наведено у табл. 1.

Таблиця 1.
Основні глобальні системи кібербезпеки

№	Система	Керівні документи (роки)
1	Стратегія кібербезпеки Організації американських держав (OAS)	Комплексна міжамериканська стратегія кібербезпеки: мультиаспектний та міждисциплінарний підхід до створення культури кібербезпеки (OAS, 2004)
2	Глобальна програма кібербезпеки (ITU- GCA)	Звіт голови Групи експертів вищого рівня (HLEG) щодо Глобальної програми кібербезпеки (GCA) MCE (Schjolberg 2007) Керівництво з національної стратегії кібербезпеки (MCE, 2012) Глобальний індекс кібербезпеки (GCI) (ITU 2017a; ITU and ABI research 2014, 2015)
3	Структура Союзу комерційного програмного забезпечення (BSA)	Глобальна система кібербезпеки BSA (BSA, 2010)
4	Принципи та керівні вказівки Всесвітнього економічного	Партнерство заради забезпечення кіберстійкості: ризик та відповідальність у гіперпов’язаному світі - Принципи та керівні

	форуму (WEF)	вказівки (WEF, 2012a). Ризик та відповідальність у гіперпов'язаному світі: шляхи до глобальної кіберстійкості (ВЕФ, 2016б). Ризик та відповідальність у гіперпов'язаному світі: значення для підприємств (ВЕФ, 2014).
5	Керівництво експертного центру спільного кіберзахисту (CCDCOE)	Керівництво по системі національної кібербезпеки (Klimburg 2012)
6	ISO 27032	ISO/IEC 27032:2012 Інформаційні технології. Методи забезпечення безпеки. Керівні вказівки по кібербезпеці (ISO/IEC 2012)
7	Стратегія кібербезпеки ЄС	Національні стратегії кібербезпеки: практичне керівництво з розробки та реалізації (ENISA 2012a). Стратегія кібербезпеки ЄС: відкритий, безпечний та надійний кіберпростір (ЄС 2013).
8	Керівництво з кібербезпеки Microsoft	Розробка національної стратегії кібербезпеки: основи безпеки, ріст та інновації (Microsoft 2013)
9	Nexus для кібербезпеки від ISACA	Трансформація кібербезпеки (ISAKA 2013)
10	Система Національного інституту стандартів та технологій (NIST)	Система для покращення критичної інфраструктури кібербезпеки
11	Модель спроможності та надійності розробки кібербезпеки (CMM)	Модель спроможності та надійності розробки кібербезпеки (GCSCC 2014)
12	Керівні принципи кібербезпеки Співтовариства	Підхід Співтовариства до розробки національних стратегій кібербезпеки: керівництво по створенню цілісного та всеоб'ємного підходу до створення безпечного, надійного та безвідмовного кіберпростору (СТО 2015) Модель кіберуправління Співтовариства (Commonwealth 2014)

Певні особливості та відмінності можуть бути знайдені в кожній СКБ, адже кожна СКБ у певному сенсі є унікальною. Проаналізувавши зазначені керівні документи та врахувавши зауваження експертів [1, 3-4], було визначено чотири аспекти такої унікальності, а саме: 1) заохочувані дії; 2) драйвери; 3) середовище та 4) аудиторія.

При цьому, заохочувана дія – це бажана чи рекомендована дія, що пов'язана з основним змістом СКБ; драйвер є фактором, що мотивував створення даної СКБ; середовище – це ситуаційні обставини, в яких можна використовувати СКБ; аудиторія – ймовірні користувачі СКБ.

Розглянемо зазначені аспекти докладніше.

1. Заоховувані дії. Заохочувані дії у СКБ можна поділити на два основні типи. Дії першого типу просувають колаборацію з іншими акторами (зовнішня стратегія), в той час як дії другого типу спрямовані на збільшення кіберпотенціалу певної організації, інституції, структури тощо (внутрішня стратегія).

Дії першого типу сприяють співпраці між різними акторами в кіберпросторі, посилюють їхню позитивну взаємозалежність. Основна ідея, закладена в основу цих дії, полягає у тому, що кібербезпека є загальною відповідальністю, а виникаючі проблеми пов'язані зі взаємозалежностями всіх зацікавлених сторін у кіберпросторі. Цей тип включає такі СКБ, як ISO/IEC 27032, Принципи та керівні вказівки WEF, Глобальна повістка денна по кібербезпеці ITU, Стратегія кібербезпеки OAS та Керівництво по кібербезпеці СТО.

На відміну від дій, орієнтованих назовні, інший тип заохочуваних дій підтримує внутрішні процеси та сприяє внутрішньому укріпленню організації (інституції, структури) шляхом створення/збільшення кіберпотенціалу. В той час як заохочувані зовнішні дії спрямовані на спільну боротьбу з кіберзагрозами, для організації (інституції, структури) також важливо мати достатню кіберспроможність, щоб бути надійним та сильним самостійним актором. З цієї причини, деякі СКБ, такі як Oxford University CMM та система NIST, виступають за посилення організаційного потенціалу, наприклад, шляхом нарощення потенціалу людських ресурсів, укріплення критично важливих інформаційних інфраструктур та зміцнення внутрішніх систем (тобто нормативних актів, правил та організаційної структури).

2. Драйвери. Як показує аналіз СКБ, стратегія кібербезпеки може визначатися двома загальними драйверами: ризиком та цінностями. Орієнтовані на ризик або на цінності драйвери здійснюють значний вплив на дії та загальну розробку стратегії кібербезпеки. Але у той час, коли деякі СКБ роблять акцент на попередженні ризиків, пов'язаних з кіберзагрозами, інші рекомендують зосередитись на узгодженні цінностей організації (інституції, структури) зі стратегією кібербезпекиУ такому ціннісно-орієнтованому контексті, створення кіберполітики означає розгляд кіберпростору не лише як ізольованого домену, а й як сфери, що включає політичну ситуацію та загальну національну стратегію розвитку (Klimburg 2012). Тому,

захист кіберпростору має зважати також і на політичні чинники. Всередині приватної організації це може прийняти форму узгодження бізнес-стратегії зі стратегією безпеки, що означає додавання функції кібербезпеки на основі бізнес-середовища, бізнес-цілей та цілей безпеки (ISACA 2013; NIST 2014).

СКБ, що містять орієнтовані на цінність драйвери, можна знайти, в першу чергу, в IGO СКБ, таких як Керівні принципи Стратегії кібербезпеки Співдружності, Стратегія кібербезпеки ЄС, Структура кібербезпеки CCDCOE та ITU-GCA, де основним є намір просувати свої інституціональні цінності (сприяння стратегії кібербезпеки, демократичне та ефективне управління, міжнародне співробітництво, нарощення потенціалу тощо).

3. Середовище. Неможливо впроваджувати та розвивати СКБ, реалізовувати стратегії з кібербезпеки не розуміючи їх зовнішнє середовище. При цьому слід зважати на те, що деякі системи покликані забезпечити відповідні результати на організаційному рівні, а інші призначені для використання на регіональному або міжнародному рівні (що вимагає позитивної взаємозалежності між міжнародними кіберорганізаціями). Зовнішнє середовище СКБ можна поділити на три рівні: організаційний, регіональний та міжнародний. Організаційний рівень, як правило, стосується підвищення потенціалу організації, тоді як інші два мають на меті забезпечення позитивної взаємозалежності різних суб'єктів у сфері кібербезпеки. При цьому організаційна система може використовуватися як система, що доповнює системи вищого рівня, тому організація може також впроваджувати ще одну систему високого рівня поряд із системою організаційного типу. Регіональна система, як правило, будується для задоволення конкретних потреб країн-членів, які мають подібні спільні інституційні цінності. Натомість міжнародні системи, підкреслюючи важливість позитивної взаємозалежності, що має характер кооперації, сприяє встановленню співпраці будь-яких організацій і структур, що мають аналогічні інтереси.

4. Аудиторії. Відповідно до аудиторії або передбачуваних користувачів СКБ можна розділити на два типи: 1) СКБ, орієнтовані на специфічну аудиторію; 2) СКБ, орієнтовані на загальну аудиторію.

СКБ першого типу, як можна бачити з назви, створені для конкретного типу аудиторії. Наприклад, система NIST була розроблена у відповідь на Указ Президента США № 136362 від 11.05.2017 р., оскільки ця система була спочатку побудована для оператора критичної інформаційної інфраструктури в США. Другий тип СКБ має загальну застосовність щодо своєї аудиторії та зосереджений на наданні організаціям і структурам можливості збільшити їхню спроможність зменшити кіберзагрози; їх може використовувати будь-яка організація та структура, оскільки вони не прив'язані до конкретної місії. Цей тип СКБ зазвичай будують НУО та академічні установи, такі як Оксфордський університет, ISO/IEC, Microsoft або BSA.

Таким чином, кожну СКБ можна охарактеризувати, віднісши її до певного типу за категоріями: заохочувані дії – позитивна незалежність або збільшення потенціалу; драйвери – орієнтовані на ризик або орієнтовані на цінності; середовище – організаційне, регіональне або міжнародне; аудиторія – специфічна або загальна. Але у той же час, СКБ можуть мати і демікласифікацію, що означає проміжне положення між декількома категоріями. Однак принципи, закладені у цих СКБ, можуть бути прийняті глобально будь-якою організацією.

Хоча існують різні точки зору на сутність і зміст СКБ, також існують і загальні моменти, притаманні більшості СКБ. І, насамперед, це стосується тих понять, що використовуються для опису побудови і розвитку СКБ. Проаналізувавши багато як концептуальних документів, про які йшлося вище, так і наукових джерел, визначено спільні поняття, що зустрічаються у багатьох з них і стосуються забезпечення кібербезпеки в органах публічної влади. Зазначені основні поняття запропоновано далі поділити на дві групи, відповідно до їх змісту: 1) виміри кібербезпеки; 2) дії, необхідні для забезпечення кібербезпеки в органах публічної влади. Далі слід описати концептуальні засади забезпечення кібербезпеки в органах публічної влади більш детально.

До першої групи віднесено п'ять вимірів кібербезпеки: людський, організаційний, інфраструктурний, технологічний, нормативний. А до другої групи належать такі заходи: побудова довіри в Інтернеті, створення координації, співпраці та сумісної роботи, профілювання кібердержави, сприяння впровадженню, аналіз, встановлення правового середовища та створення стандартів. Розглянемо їх.

Важливим є питання щодо вимірів кібербезпеки.

Людський вимір є найбільш фундаментальним і, можливо, найбільш слабким елементом кібербезпеки. Хоча кіберпростір побудований на технологіях, людина управляє ними і контролює їх. Оскільки люди є основними акторами, що забезпечують кібербезпека, недостатня поінформованість і недостатні знання роблять людей головною проблемою і найбільш вразливою ланкою в порівнянні з іншими. Крім того, вирішення проблеми нестачі знань не є простим завданням, оскільки вимагає навчання та підготовки протягом певного часу. З цієї причини СКБ рекомендують посилення кібербезпеки шляхом підвищення обізнаності, розвитку культури кібербезпеки, а також забезпечення навчання осіб, які займаються питаннями кібербезпеки.

Організаційний вимір зосереджений на інститутах всередині кіберпростору. Це функціональна структура, яка контролює кіберпростір. Зміцнення цього виміру може відбуватись за двома напрямами: 1) стратегічні дії орієнтовані всередині країни, такі як підвищення потенціалу і можливостей відповідної структури; 2) стратегічні дії орієнтовані назовні, які активізують співпрацю для забезпечення безпеки кіберпростору. Наприклад, перший напрям може бути реалізований шляхом забезпечення необхідних ресурсів для організації та підвищення реагування на кіберзагрози. Однак, кожна організація в кіберпросторі

також повинна співпрацювати з іншими, наприклад, шляхом визначення чітких ролей і обов'язків для кожної організації, координації дій, обміну інформацією про загрози і створення альянсів і партнерств.

Інфраструктурний вимір є, мабуть, найбільш важливим елементом кіберпростору. Це середовище, яке створює кіберпростір. Без інфраструктури кіберпростір – ніщо, тому зміцнення цього виміру необхідно для підтримки кіберсередовища у цілому. Якщо цей вимір слабкий, транзакції в кіберпросторі можуть суттєво знизитись. Тому більшість СКБ звертають особливу увагу на інфраструктурні проблеми, у тому числі, на способи забезпечення безпеки критично важливої інформаційної інфраструктури. У цьому сенсі, структура NIST є найбільш придатною для захисту критично важливої інформаційної інфраструктури, але у більшості випадків системи захисту такої інфраструктури відрізняються у різних організаціях, залежно від потреб кожної організації та відповідного кіберпрофілю.

Технологічний вимір розширює можливості кіберпростору. Оскільки кіберпростір включає в себе найбільш передові технології, зміцнення цього виміру в першу чергу означає впровадження новітніх та найбільш ефективних технологій, що забезпечують кібербезпеку і дозволяють проводити подальші дослідження і розробки у цій сфері.

Нормативний вимір структурує кібербезпеку і створює певне імперативне середовище у кіберпросторі. Цей вимір спрямований на формування національної кіберекосистеми шляхом створення нормативно-правової бази та розробки норм і стандартів, а також правозастосування. Хоча деякі стверджують, що кіберпростір не повинний регулюватися і має залишатися вільним від втручання органів влади та політики (Barlow, 1996), правова поведінка все ж необхідна для підтримки стабільності в кіберпросторі.

Цікаво порівняти визначені нами виміри з тими, що їх визначає ITU (International Telecommunication Union) і які вважаються багатьма авторами як певні еталони у цій сфері. ITU також визначає п’ять вимірів, але дещо інших: 1) правовий; 2) технічний і процедурний; 3) організаційний; 4) створення потенціалу; 5) міжнародне співробітництво.

Як можна бачити, чотири з п’яти вимірів ITU, – технічний і процедурний, організаційний та міжнародне співробітництво, – можуть бути охоплені організаційним виміром. Як зазначалось, організаційний вимір виступає в якості функціональної структури, що контролює кіберпростір, та передбачає внутрішні стратегічні дії (підвищення потенціалу і можливостей організації, що охоплює такі виміри ITU, як технічні та процедурні, організаційні та створення потенціалу); і зовнішні стратегічні дії (розширення співпраці в цілях забезпечення безпеки в кіберпросторі, що відповідає міжнародному співробітництву ITU).

Натомість, є певні основні виміри, запропоновані в цьому дослідженні, які не визначаються ITU – інфраструктурний і технологічний, а людський вимір хоча і згадується, але не визначається як окремий. Таким чином, запропонована класифікація вимірів є більш повною і точною.

Успішність запобігання кіберзлочинам, їх викриття та притягнення винних осіб до відповідальності наразі є «достатньо рідкісним явищем, якщо порівнювати з кількістю таких правопорушень» [2, с. 3]. Отже, науковий інтерес також має надання рекомендацій щодо переліку дії, необхідних для забезпечення кібербезпеки, до яких віднесено:

1) Створення онлайн-довіри. При створенні стратегії кібербезпеки, деякі СКБ рекомендують, щоб при розробці політики основну увагу було приділено підвищенню довіри зацікавлених сторін до онлайн-середовища чи створення онлайн-довіри. Це означає не лише представлення зацікавленим сторонам (наприклад, споживачам, бізнесу та уряду) упевненості в онлайн-формі, а також забезпечення доступності інфраструктури. Це може бути досягнуто, наприклад, шляхом забезпечення системи захисту даних та регулювання конфіденційності, розробки національного плану регулювання в надзвичайних ситуаціях в кіберпросторі, управління національними кризами та забезпечення захисту критично важливої інформації.

Найчастіше створенню довіри в Інтернеті сприяють:

– збільшення цифрової надлишковості.

– захист важливих активів в кіберпросторі (таких як конфіденційність, дані та інфраструктура);

– просування конфіденційності в Інтернеті: для захисту приватної інформації від несанкціонованого доступу та розголошення.

2) Координація, співпраця та кооперація. Враховуючи широкий спектр необхідного захисту кібербезпеки, включаючи захист на особистому, суспільному, організаційному, національному та міжнародному рівнях, а також захист глобального кіберпростору, він не може бути здійснена лише одним суб’єктом. Такий захист потребує співпраці зі сторони кожного суб’єкта, і, крім того, кіберпростір потребує кумулятивного захисту. Це означає, що кожен об’єкт повинен постійно працювати над підтримкою (та покращенням) своєї кіберспроможності, щоб бути надійним гравцем в такій системі.

Існує два типи рекомендованих дій по координації, співпраці та кооперації (ССС). Можемо розділити дії, пов’язані з організаційними відношеннями, на зовнішні та внутрішні дії. Перша категорія включає в себе взаємодію з іншими організаціями шляхом співпраці та взаємодії. Інформаційно-пропагадистська діяльність може бути досягнута, наприклад, шляхом альянсів та партнерських відносин з іншими організаціями, розширення можливостей кібернетичної дипломатії та м’якої сили, обміну інформацією стосовно боротьби з загрозами, поділу відповідальності шляхом заохочення інтеграції та збільшення кібер-потенціалу сусідських організацій (чи впровадження третіми сторонами).

Друга категорія включає в себе підвищення внутрішньої координації в рамках організаційної структури організації. Цей тип дій призначений для покращення зв'язку з усіма зацікавленими сторонами організації, координації всіх зацікавлених сторін організації по відношенню до мандата кібербезпеки та створення кіберуправління з чіткими ролями та обов'язками.

3) Профілювання кіберстану. Дія профілювання включає в себе постановку цілей і пов'язаних ресурсів, які необхідні для захисту кіберпростору, що є попередніми підготовчими діями перед початком наступного дії. До складу профілювання кібернетичного стану входять три дії: приведення стратегії у відповідність з основними цінностями; складання бюджету та підготовка відповідних ресурсів; і формулювання припущень.

4) Стимулювання прогресу, що спрямоване на сприяння впровадженню СКБ. Це означає збільшення кіберпотенціалу організації шляхом сприяння прийняттю принципів роботи СКБ. На додаток до ССС, також важливо розглянути дії по відношенню до інших об'єктів в кіберпросторі. Стимулювання прогресу може вважатися важливим аспектом цих відносин, тому що для зміцнення кібербезпеки принципово бути довіреною організацією в кіберпросторі. Дії КТС і сприяння впровадженню взаємопов'язані. У той час як ССС відображає зовнішні дії зі співпраці з усіма організаціями та зацікавленими сторонами, основною метою сприяння впровадженню є внутрішньо спрямовані стратегічні дії щодо зміцнення організації з тим, щоб їй довіряли в кіберпросторі (WEF 2012b). Такі дії можуть приймати форму підвищення обізнаності, створення кіберкультури, інвестування в дослідження та інновації, використання інноваційних технологій, підвищення реагування на кібернетичні процеси, а також навчання і освіти в області кібербезпеки.

5) Огляд та рецензування. Діяльність, яка здійснюється для захисту кіберпростору, також має бути переглянута, щоб гарантувати виконання своїх завдань програмою кібербезпеки. Рецензування призначене для коригування стратегії і перебудови програми для досягнення наміченої мети. Приклади таких дій включають створення аудитів і журналів, отримання зворотного зв'язку, проведення самооцінок і уточнення програми. Крім створення аудитів і журналів, необхідно також оцінити дію. Оцінка програми можна проводити всередині країни або із залученням зовнішнього спостерігача.

6) Створення правового середовища. Правове середовище забезпечує основу для поведінки в кіберпросторі, яке встановлює межу між тим, що допускається, і тим, що є проступком. Для запобігання і припинення неправомірних дій необхідні відповідні закони і правила. Більшість СКБ радять організації визначити, що таке правова поведінка, і створити правове середовище. Створення правового середовища припускає створення правової основи як основи для розмежування легальної та нелегальної діяльності в кіберпросторі. Створення правового середовища також може бути використано в якості обґрунтування для прийняття коригувальних заходів проти зловмисних дій в кіберпросторі. Визначення політики означає створення юридичного обґрунтування поведінки. При визначенні такої політики СКБ рекомендують враховувати деякі аспекти:

– визнавати природу Інтернету, означаючи, що він повинен зберігати відкритість і вільний потік інформації;

– слідувати сучасним тенденціям з усіма аспектами сучасної кіберзлочинністю діяльності;

– заохочувати співпрацю і розроблятися з використанням існуючих міжнародних та регіональних структур в якості довідкових.

– політика повинна використовуватися для мінімізації ризику та як форми стримування неправомірного використання.

Реалізація політики має створити стратегію і структуру, тобто вона повинна розробити стратегію, механізм і дорожню карту, які функціонують як тактичний або навіть прямий мандат щодо захисту кіберпростору.

7) Створення стандартів. Захист кіберпростору вимагає ефективних і дієвих дій, які можуть бути реалізовані шляхом прийняття найкращих практик та стандартизації поведінки. Це може бути досягнуто шляхом створення стандарту, який також означає сприяння взаємодії та систематизацію поведінки. Сприяння функціональної сумісності означає слідування визнаним міжнародним стандартам кібербезпеки. Організації можуть також стандартизувати свою поведінку, розробивши і встановивши мінімальні вимоги до поведінки. Прикладом цього є створення практичних і ефективних програм реалізації і технічних керівних принципів. Ця дія спрямована на мінімізацію дублюючих дій між одним об'єктом і іншими.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. У пошуках політики в області кібербезпеки, варто відзначити один цікавий питання, що рухає її розвитком. Це питання приводить до розуміння ініціатив організацій по розробці СКБ через усвідомлення відмінних рис СКБ. Аналіз організаційних основ документів з регулювання кібербезпеки дозволив визначити мету загальних концепцій по 12 СКБ та класифікації їх відмінностей. Використовуючи засновану на теорії парадигму, було розділено СКБ на дві основні частини: контекст та загальні концепції. У цьому дослідженні виявлено, що розвиток СКБ може в цілому відображатися:

1) заохочуваними діями (позитивна взаємозалежність в порівнянні зі збільшенням потенціалу),
2) рушійною силою (кібер-ризик проти просування цінностей),
3) системним середовищем (організаційне, регіональне і міжнародне),
4) аудиторією (специфічна та загальна СКБ).

Крім того, розуміння СКБ як нормативної концепції є постійним завданням. Як зазначено в роботі

[5, с. 29], існує бажання розробити загальні стратегії, які можуть застосовуватися на глобальному рівні, наприклад шляхом створення інструментарію кібербезпеки. Таким чином, вирішення питання, яке веде до розробки загальних концепцій кібербезпеки, сприяє розробці загальної моделі політики кібербезпеки.

Намагаючись відповісти на цей запит, це дослідження зіставило нормативну позицію СКБ з трьома основними концепціями, які охоплюють сім тем дій, п'ять компонентів/ об'єктів та трьохпроцесний життєвий цикл. Сім тем дій, які часто обговорюються в СКБ, а саме:

- побудова довіри в Інтернеті;
- координація, співпраця і кооперація;
- профілювання кібернетичного стану;
- сприяння впровадженню;
- огляд та рецензування;
- створення правового середовища та системи стандартів.

Також розглянуто п'ять компонентів або об'єктів кібербезпеки, які найчастіше обговорюються в СКБ, а саме: людина, організація, інфраструктура, технології та законодавство і регулювання.

Слід зазначити, що реалізація проекту з кібербезпеки у сфері публічного управління не проста, вона включає постійне поліпшення, моніторинг та аналіз, а отже доречним стає питання щодо діагностики та подальшого врахування життєвого циклу системи кібербезпеки, що й заплановано обрати у якості перспективного напряму подальших досліджень.

Список літератури.

1. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174-180.

2. Нікулеску Д. Кібербезпека: вразливі моменти // Юридична газета online (2019). URL: http//yur-gazeta.com/publcations/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення 15.01.2020 р.).

3. Azmi R., Tibben W., Than Win K. Review of cybersecurity frameworks: context and shared concepts // Journal of cyber policy, 2018. URL: https://doi.org/10.1080/23738871.2018.1520271 (дата звернення 24.12.2019 р.)

4. Bowen, G. A. Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 2009, p. 27-40. doi:10.3316/qrj0902027 (дата звернення 07.06.2019 р.).

5. House W. Cyberspace Policy Review: Assuring a Trusted and Resiliant Information and Communications Infrastructure. June 2009. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. (дата звернення 04.02.2020 р.).

References.

1. Lipkan, V., Diorditsa, I. (2017) “National system of ciberbezpeci how component part of the system of providing of national safety of Ukraine is” // *Pidpryemnytstvo, hospodarstvo i pravo*, vol. 5, pp. 174-180.

2. Nikulecku, D. (2019) “Ciberbezpeca: impressionable moments” // *Yurydychna hazeta online*, available at: http//yur-gazeta.com/publcations/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (Accessed 15 Jan 2020)

3. Azmi, R., Tibben, W. and Than Win, K. (2018) “Review of cybersecurity frameworks: context and shared concepts” // *Journal of cyber policy*, available at: https://doi.org/10.1080/23738871.2018.1520271 (Accessed 24 Dec 2019)

4. Bowen, G. A. (2009) “Document Analysis as a Qualitative Research Method”. *Qualitative Research Journal* 9: 27-40, available at: doi:10.3316/qrj0902027 (Accessed 7 June 2019).

5. House, W. (2009) “Cyberspace Policy Review: Assuring a Trusted and Resiliant Information and Communications Infrastructure”, available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. (Accessed 4 Feb 2020).

Стаття надійшла до редакції 24.02.2020 р.