DOI: 10.18372/2410-7840.21.13951
УДК 004.056.5:343.326 (045)

КІБЕРБЕЗПЕКА УКРАЇНИ: АНАЛІЗ СУЧАСНОГО СТАНУ

Олена Трофименко, Юлія Прокоп, Наталія Логінова, Олександр Задерейко

За умов стрімкого зростання кіберризиків і кіберзагроз важливим є моніторинг сучасного стану кібербезпеки нашої країни, висвітлення основних проблем розбудови національної системи кіберзахисту та визначення напрямів їх вирішення. При цьому потрібен як аналіз вже реалізованих заходів у сфері захисту комп'ютерних і телекомунікаційних мереж від кібератак, так і визначення потрібних для реалізації заходів щодо створення умов для безпечного функціонування кіберпростору. Проведене дослідження свідчить про вагомі політичні, економічні і соціальні зусилля з посилення кіберстійкості, які докладає держава задля розвитку національних можливостей з кібербезпеки. З'ясовано, що ефективне забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора та громадянського суспільства. У статті визначено політичні, науково-технічні, організаційні та просвітницькі питання, вирішення яких є необхідним у рамках комплексної протидії кіберзагрозам задля випереджального реагування на динамічні змінення, що відбуваються у кіберпросторі. Зазначено про доцільність докладати більше зусиль для встановлення державно-приватного партнерства, розроблення та запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі. Наголошується на тому, що Україна має активізувати свою участь в організації спільних міжнародних проектів з нарощування кібернетичного потенціалу з метою узгодження дій та пошуку нових шляхів у посиленні кібербезпеки і захисті критично важливих інформаційних інфраструктур у відповідь на нові тенденції в глобальному русі до цифрової економіки та інформаційного суспільства.
Ключові слова: *кібербезпека, кібератака, кіберінциденти, кіберзагрози, інформаційна безпека, стратегія кібербезпеки.*

Вступ

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними. Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами. Зі зростанням залежності від використання ІКТ у бізнесі і підприємництві відповідно зростають кіберризики і кіберзагрози, що потребує завчасного реагування щодо їх запобігання або вирішення та обізнаності з факторами ризику всіх зацікавлених сторін. Система кібербезпеки має працювати в інтересах громадськості як для постачальників послуг, так і для користувачів послуг. Саме держава як гарант прав і свобод громадян має взяти на себе відповідальність за забезпечення доступу до стабільного безпечного цифрового простору, яким можуть скористатися всі громадяни, адже забезпечення належного рівня кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Аналіз останніх досліджень та публікацій

Важливості питань інформаційної безпеки нашої країни і формуванню механізму міжнародної кібербезпеки приділяли увагу численні науковці. Так, Безуглий Д.С. обґрунтував необхідність інформаційної безпеки як складової частини національної безпеки країни [1]. Аналіз останніх досліджень і публікацій свідчить про те, що певні аспекти вітчизняних проблем інформаційної безпеки у той чи інший спосіб досліджувались у наукових працях Арістова І.В., Березовської І.Р., Дзьобаня О.П., Калюжного Р.А., Кормича Б.А., Ліпкана В.А., Марущак А.І., Цимбалюка В.С., Юдіна О.К. та інших. Питанням формування ефективного механізму правового регулювання протидії загрозам у кібернетичній сфері присвятили свої праці такі науковці: Сопілко І.В., Куцаєв В.В., Живило Є.О., Мінін Д.С., Шеломенцев В.П., Бурячок В.Л., Гнатюк С.О. та інші. Проте ці дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України.

Мета роботи

За сучасних умов гібридної війни побудова системи кібернетичної безпеки України вимагає чіткого аналізу вже реалізованих заходів у сфері захисту комп'ютерних і телекомунікаційних мереж від кібератак та визначення потрібних для реалізації заходів щодо створення умов для безпечного функціонування кіберпростору задля випереджального реагування на динамічні зміни, що відбуваються у кіберпросторі. Метою статті є комплексний аналіз сучасного стану кібернетичної безпеки нашої країни, висвітлення основних проблем розбудови національної системи кіберзахисту та визначення напрямів їх вирішення.

Виклад основного матеріалу дослідження

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки [12].

Задля готовності забезпечувати кібербезпеку і відбивати відкриту агресію в кіберпросторі *Україна реалізувала цілий комплекс заходів* для вирішення стратегічних, правових, політичних, технічних та організаційних питань з безпечного функціонування кіберпростору (рис. 1).

Рис. 1. Комплекс реалізованих заходів з безпечного функціонування кіберпростору станом на 2019 рік

Стратегічна політика кібербезпеки. Критичним елементом соціально-економічної безпеки будь-якої країни є Національна стратегія кібербезпеки (National Cybersecurity Strategy, NCS) [16]. Стратегію кібербезпеки України було введено в дію 27.01.2016 р. [7]. Саме в ній кібербезпека та інформаційна безпека визнані як одні з головних пріоритетів у протидії загрозам національній безпеці. Деталізацію реалізації Стратегії кібербезпеки відображено у щорічних планах уряду, в яких з боку органів влади передбачено заходи щодо запобігання і підготовки реагування на можливі кіберінциденти у рамках створення ефективної національної системи кібербезпеки.

Задля координації і контролю діяльності різних суб'єктів у царині кібербезпеки організовано роботу відповідних державних служб, за якими закріплено конкретні зобов'язання з дотримання вимог кібербезпеки:

– запроваджено певний механізм керівництва й організовано роботу Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, який безпосередньо координує міжвідомчу взаємодію суб'єктів національної безпеки і оборони України під час кібератак та кіберінцидентів в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури задля покращення ефективності си-

стеми державного управління у формуванні та реалізації державної політики у сфері кібербезпеки під час реалізації Стратегії кібербезпеки України;

– функції державного контролю у сфері боротьби з кіберзлочинністю, кіберзахисту об'єктів критичної інформаційної інфраструктури, формування та реалізації державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації покладено на Державну службу спеціального зв'язку та захисту інформації України (ДССЗЗІ). Саме вона координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту і здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти й кібератаки та усунення їх наслідків. ДССЗЗІ забезпечує функціонування урядової Команди реагування на комп'ютерні надзвичайні події України (CERT-UA) та Державного центру кіберзахисту, який здійснює впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки. Ядром цієї моделі є Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC), створений 02.02.2018 р. як центральний компонент національної системи кіберзахисту України. CRC побудовано на базі найновітніших досягнень у сфері кібербезпеки як вітчизняних, так і провідних IT-компаній світу. Розроблені на рівні кращих світових аналогів сучасні технологічна та аналітична системи CRC закономірно претендують на звання найпотужніших в європейському співтоваристві [13]. Інша важлива функція ДССЗЗІ пов'язана з контролем за дотриманням вимог законодавства у сфері електронних довірчих послуг, наглядом за кваліфікованими постачальниками електронних довірчих послуг, у галузі криптографічного захисту інформації [4]. Адже саме гарантування конфіденційності й цілісності інформації, захист інформації від несанкціонованого доступу є вимогою успішної реалізації електронного документообігу між державними установами, громадянами та суб'єктами приватного сектора;

– оскільки сьогодні персональні дані громадян потребують захисту так само, як і конфіденційні дані компаній, в Україні був створений відповідний незалежний державний наглядовий орган, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованим обробленням персональних даних. Контроль за дотриманням законодавства про захист персональних даних було покладено на Уповноваженого Верховної Ради України з прав людини [14];

– організовано роботу Департаменту кіберполіції Національної поліції України, який спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних мереж і систем [6];

– створено компетентний орган у сфері інформаційної безпеки – Державне агентство з електронного врядування України [3], яке має повноваження контролювати операторів основних послуг щодо вимог кібербезпеки.

Постачальників цифрових послуг та операторів основних служб відповідно до ст. 5 Закону України про кібербезпеку зобов'язали керувати кіберризиками, реалізовувати у межах своєї компетенції заходи для забезпечення кібербезпеки і повідомляти відповідні державні органи про випадки кіберінцидентів.

Прийняття відповідного законодавства. Слід зазначити, що в Україні законодавча ситуація з кібербезпеки після 2014 року набула значних зрушень. Станом на 2019 рік сформовано законодавчу базу у сфері кібербезпеки держави [10]: затверджено Доктрину інформаційної безпеки України (введена в дію 25.02.2017 р.), закони України «Про основні засади забезпечення кібербезпеки України» 2163-VIII (набрав чинності 09.05.2018 р.), «Про національну безпеку України» 2469-VIII (набрав чинності 08.07.2018 р.), «Про інформацію» 2657-XII (редакція від 01.01.2017 р.), «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР (редакція від 19.04.2014 р.), «Про електронні довірчі послуги» 2155-VIII (набрав чинності 07.11.2018 р.), «Про захист персональних даних» 2297-VI (редакція від 30.01.2018 р.) тощо. Низка відповідних положень щодо кібербезпеки закріплена в указах президента, зокрема: «Про Концепцію розвитку сектора безпеки і оборони України» (№ 92/2016 від 14.03.2016 р.); «Про стратегічний оборонний бюлетень України» (№ 240/2016 від 06.06.2016 р.), «Про Національний координаційний центр кібербезпеки» (№ 242/2016 від 07.06.2016 р.) тощо.

Саме Закон «Про основні засади забезпечення кібербезпеки України» визначає основні об'єкти кіберзахисту, які створюють критичну інфраструктуру країни, нормативно закріплює понятійний апарат у сфері кібербезпеки на найвищому рівні, регламентує принципи забезпечення кібербезпеки та національну систему кібербезпеки, окрес-

лює державно-приватну взаємодію у сфері кібербезпеки та встановлює відповідальність за порушення законодавства у цій сфері і контроль за законністю заходів щодо забезпечення кібербезпеки України [7].

Глобальне партнерство. Задля поглиблення міжнародного співробітництва і гармонізації нормативних документів у сфері кібербезпеки, відповідно до міжнародних стандартів і стандартів ЄС та НАТО, Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші міжнародні договори.

За підтримки трастового фонду НАТО створено Ситуаційні центри [9] при СБУ та ДССЗЗІ, на які покладено завдання з виявлення, запобігання та нейтралізації акцій кібернетичного характеру проти України. Завдяки цьому в Національній поліції України діє Національний контактний пункт формату 24/7 щодо реагування та обміну інформацією про комп'ютерні злочини.

З метою посилення стійкості критичної національної інфраструктури з кібербезпеки український Уряд регулярно бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів реагування на кіберінциденти. Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС та НАТО посилюють спроможності України у сфері кібербезпеки і відповідають національним інтересам.

У рамках взаємодії з міжнародними організаціями з питань реагування на кіберінциденти було організовано участь України у Форумі команд реагування на інциденти інформаційної безпеки FIRST (Forum for Incident Response and Security Teams), що об'єднує різні групи CERT (Computer Emergency Response Team – Команда реагування на надзвичайні ситуації) у країнах Європи.

Просвітницькі програми з кібербезпеки. Позаяк кіберзагрози неможливо обмежити якоюсь однією сферою, це вимагає від усіх зацікавлених сторін всебічної обізнаності з факторами ризику, умінь і навиків для їхнього вирішення та відповідних заходів для запобігання кібератак ще до їх початку. Україна активно залучає провідні організації до підвищення ступеня обізнаності комерційних підприємств і неприбуткових організацій щодо кібербезпеки на всіх рівнях.

Організовано роботу підрозділу CERT-UA – Державного центру захисту інформаційно-телекомунікаційних систем (ДЦЗ ІТС) ДССЗЗІ, який спеціалізується на виявленні кіберінцидентів та реагуванні на них. CERT-UA на своєму сайті https://cert.gov.ua/ демонструє вразливі до зламу місця стандартного периметру охорони даних, надає рекомендації мінімізації ризиків та технічну допомогу з подолання наслідків кібератак. Команда CERT-UA у співпраці з іншими групами країн-членів CERT не лише вживає заходів з виявлення причин та обставин кіберінцидентів у критичній інформаційній інфраструктурі, а й допомагає усунути загрози для приватного та іноземного секторів. До речі, Закон України «Про основні засади кібербезпеки України», серед іншого, визначає завдання CERT-UA на законодавчому рівні. Відповідно до цього Закону, CERT-UA та Центр реагування на кіберзагрози відіграватимуть координуючу роль у заходах, спрямованих на оперативну (кризову) реакцію на кібератаки та кіберінциденти, а також у запровадженні контрзаходів, спрямованих на мінімізацію вразливості систем зв'язку.

Організовано роботу Київського відділення всесвітньовідомої організації з розроблення методології та стандартів у галузі управління, аудиту і безпеки інформаційних технологій ISACA (Information Systems Audit and Control Association, http://www.isaca.org). Об'єднуючи учасників 180 країн світу, ISACA пропонує фахівцям з кібербезпеки широкий спектр ресурсів, що допомагають організаціям в управлінні та контролі за інформацією і технологіями [2].

В Україні у різних вищих навчальних закладах активно запроваджуються просвітницькі навчальні програми з кібербезпеки, орієнтовані на бакалаврський, магістерський або професійний рівень.

Отже, проведене дослідження свідчить про вагомі політичні, економічні і соціальні зусилля з посилення кіберстійкості, які докладає держава задля розвитку національних можливостей з кібербезпеки, навіть за умов великої кількості кібератак. Аналіз показує, що у разі продовжування та активації започаткованої трансформації протягом двох-трьох років можна досягти стійкого рівня кіберстійкості, де безпека стане «звичайним бізнесом», вбудованим у структуру організацій. Забезпечення кібербезпеки можливе тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації. Розглянемо політичні, технічні та організаційні питання, вирішення яких є необхідним у рамках комплексної протидії кіберзагрозам.

Політичний рівень. Серед першочергових завдань, які стоять перед державними інститутами України в рамках забезпечення інформаційного та цифрового суверенітетів, є: здійснення автоматичного моніторингу свого інформаційного простору; впровадження законодавства про відповідальність за контент; впровадження законодавства, яке регулює фільтрацію інтернет-контенту; недопущення використання новітніх інформаційних технологій для поширення соціально шкідливих ідей і закликів (расизму, шовінізму, радикального націоналізму); правовий захист національної культури і мови від впливу домінуючих в інформаційному плані країн; знаходження соціально прийнятного балансу між свободою слова і поширенням інформації та невід'ємним правом держави забезпечувати незалежну політику; захист від культурної експансії зарубіжних інтернет-ресурсів; перехід державних установ на використання програмного та технічного забезпечення власної розробки і виробництва [5].

Приділяти увагу треба аналізу національної стратегічної ситуації кіберзагроз, агрегувати та розповсюджувати дані про відповідні інциденти для більш ефективного реагування, на регулярній основі, принаймні раз на рік, формувати громадські звіти про кіберзагрози зі своєчасною публікацією на відповідному вебсайті.

Схвалення потребує до цього часу не прийнятий Закон «Про критичну інфраструктуру та її захист», відсутність якого нині ускладнює регулювання діяльності державного та недержавного сектора безпеки та охорони, і не лише у межах правового регулювання інституту критичної інфраструктури. До того ж, прийняття цього закону стане виконанням Резолюції Ради Безпеки ООН 2341 від 13.02.2017 р. «Про захист об'єктів критичної інфраструктури від терористичних атак» [17], яка була прийнята за ініціативи України. Метою цієї Резолюції є підвищення ефективності міжнародних зусиль та комплекс мір з реалізації національних програм боротьби з тероризмом, зокрема в рамках Глобальної контртерористичної стратегії ООН.

Задля розвитку потенціалу сектора безпеки і оборони у сфері забезпечення кібербезпеки потрібно розроблення та впровадження ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз в інформаційному просторі.

Міжнародне співробітництво. З метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях країна має активізувати участь в організації спільних міжнародних проектів з нарощування кібернетичного потенціалу.

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, які здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО. Досвід України дозволяє їй бути не лише реципієнтом допомоги від ЄС і НАТО, а й джерелом нових знань, навичок і способів протидії сучасним кіберзагрозам [9].

Сучасні інформаційні загрози підкреслюють нагальну потребу у співпраці між державами для попередження постійних загроз в інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки, адже сучасні суспільства глобально взаємопов'язані, а кібератаки можуть призвести до значних економічних і соціальних збитків. Саме тому міжнародні зусилля у посиленні кібербезпеки та захисту критично важливих інформаційних інфраструктур мають бути узгоджені та діяти у відповідь на ці нові тенденції в глобальному русі до цифрової економіки та інформаційного суспільства.

Просвітницька діяльність з кібербезпеки. Важливо підвищувати рівень обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання освітніх програм з комп'ютерної безпеки.

У сфері інформування громадськості варто розробляти та впроваджувати навчальні програми з комп'ютерної безпеки не лише у вищій школі, а й у початковій та середній освіті.

За умов небезпеки, що склалися нині у кіберпросторі, організаціям потрібно змінити ставлення до кібербезпеки. А для цього треба підвищувати обізнаність про важливість інвестування у кібербезпеку як невід'ємну складову будь-якої національної стратегії розвитку ІКТ.

Компаніям потрібно заохочувати своїх працівників до навчання кібербезпеці, створювати власні кіберталанти, рухати суспільний діалог у напрямку підвищення кваліфікації у сфері кібернавичок у більш ранньому віці, оскільки дефіцит кібернавичок тільки продовжуватиме зростати.

Організаційний рівень. За нинішньої політичної ситуації вкрай важливо посилити кібербезпеку виборчих систем та критичної інфраструк-

тури, сприяти реалізації Стратегії кібербезпеки України, посилювати реагування на кіберінциденти.

Доцільно докладати більше зусиль для встановлення державно-приватного партнерства, розробленню та запровадженню механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі. Задля своєчасного реагування на кіберінциденти і здійснення практичних заходів зі зміцнення володіння ситуацією у кіберпросторі важливо організовувати проведення тренінгів з підготовки висококваліфікованих фахівців у галузі кібербезпеки та цифрової криміналістики із залученням міжнародних фахівців.

Критично важливі інфраструктурні компанії мають дотримуватись принципу «безпека понад усе» (security-first thinking). Оскільки понад 90% усіх несанкціонованих доступів, уражень і атак відбувається через людський фактор, то на підприємствах потрібно ввести прості регламентні норми, щоб максимально мінімізувати можливі витоки загроз і уражень.

Науково-технічний рівень. Потрібні координація і переорієнтація наукових досліджень і розробок у сфері комп'ютерної безпеки, в області вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробленні технологій комплексного захисту апаратних і програмних платформ, технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливий напад і локалізацію джерела нападу [11].

Для захисту цифрових даних і послуг провайдери цифрових послуг повинні впроваджувати технології з дотримання вимог кібербезпеки та стандартів інформаційної безпеки. ДССЗЗІ як компетентний орган у сфері інформаційної безпеки має здійснювати нагляд за державними і приватними постачальниками цифрових послуг щодо дотримання вимог кібербезпеки. З метою регулярного моніторингу заходів безпеки оператори основних послуг мусять регулярно надавати докази ефективного впровадження політики інформаційної безпеки (наприклад, результати аудиту та звітну документацію).

Нові покоління програмно-апаратного забезпечення повинні бути оснащені сильнішими та зручнішими вбудованими засобами захисту. Слід підвищувати рівень безпеки комп'ютерних мереж, які використовуються для роботи з секретними даними.

Приділяти увагу треба розвитку безпечної і повсюдної електронної ідентифікації (eID), що полегшить транскордонне використання онлайн-послуг та створить умови для інтеграції України у світовий електронний інформаційний простір. Оскільки найгострішим питанням надання електронних послуг провайдерами різних сфер на сьогодні є питання захисту персональних даних споживачів таких послуг, слід посилити контроль за дотриманням вимог законодавства щодо унеможливлення доступу зловмисників до конфіденційних даних споживачів та забезпечення анонімності при eID за рахунок впровадження новітніх технічно-програмних рішень реалізації електронних транзакцій.

З масовим розповсюдженням технології інтернету речей, переходом у хмарні сховища даних, формуванням обліку FinTech, зокрема цифрових та криптовалют, криптобірж, електронних виборів та «розумних контрактів», для зниження небезпечних вразливостей треба ретельно захищати метадані від можливого викрадення унаслідок зловмисних атак.

Нині критично важливі інфраструктурні компанії відстають у підготовці своїх операційних можливостей для протистояння кібератакам. Це робить їх легкою здобиччю для політично мотивованих нападників. Такі рішення, як цифрові підписи та шифрування, доступні для надійних пристроїв ідентифікації, можуть допомогти вирішити цю проблему.

Згідно з останніми дослідженнями [15], відсоток комп'ютерів, заражених шкідливими програмами, в Україні один з найвищих у світі і складає 28,7%, тобто кожний третій комп'ютер інфікований шкідливими програмами. За таких умов вкрай важливим є обов'язкове використання комплексу програмних і апаратних засобів, які б дозволили забезпечити прийнятний рівень захищеності інфраструктури, а саме: ефективне надійне антивірусне програмне забезпечення, системи запобігання вторгнень, міжмережеві екрани, модулі контролю пристроїв і доступу до інтернету, системи шифрування даних, керування роботою мобільних пристроїв, засоби для захисту поштових серверів і систем колективної роботи тощо. Регулярне тестування на проникнення і перевірка конфігурацій (своїми силами або за допомогою зовнішніх організацій) дозволять виявити помилки в конфігураціях до того, як хакери віднайдуть доступ до управління сервером або комп'ютером користувача.

Організаціям доцільно фінансувати та впроваджувати проривні технології автоматизованого захисту, які підтримуватимуть автоматизовані можливості управління та розширену поведінкову аналітику. Прикладами цього можуть бути технології штучного інтелекту для аналізу біометричних ідентифікаційних даних, складні алгоритми машинного навчання, здатні створювати профіль типової поведінки користувача, визначати незвичні закономірності діяльності та виявляти потенційні загрози в режимі реального часу, перш ніж зловмисники матимуть можливість реалізувати їх. Завдяки автоматичній ідентифікації підозрілих даних, увесь процес дотримання безпеки стане більш ефективним, а сама кібербезпека позбавиться потреби в кропіткому ручному огляді журналу даних. Досвід показує [2], що інвестиції у кібербезпеку окупаються і навіть дають своєрідні дивіденди, позаяк дозволяють уникнути неминучої шкоди і наслідків, завдяки чому організації виходять у бізнес-лідери, а завчасні витрати є нижчими, ніж активне інвестування після атак або злочинних дій.

Висновки

Дослідження показало, що проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства. З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту у рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кібернетичній сфері, випереджальному реагування на динамічні зміни, що відбуваються у кіберпросторі, розробленню та впровадження ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі.

ЛІТЕРАТУРА

[1]. Д. Безуглий, "Інформаційна безпека України: огляд останніх тенденцій", *Фізико-математична освіта*, вип. 2(16), С. 13-17, 2018.

[2]. Впровадження європейської кібербезпеки: загальний огляд. *ISACA*. [Електронний ресурс]. Режим доступу: https://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf.

[3]. Державне агентство з електронного врядування України. [Електронний ресурс]. Режим доступу: https://www.e.gov.ua/ua.

[4]. Завдання Держспецзв'язку. [Електронний ресурс]. Режим доступу: http:// www.dsszzi.gov.ua/ dsszzi/ control/uk/publish/article?art_id=89831& cat_id=89828.

[5]. А. Задерейко, А. Троянський, Н. Логинова, Е. Трофименко, "Проблемные аспекты защиты информационного суверенитета Украины", *Інфокомунікації – сучасність та майбутнє: матер. 7 міжнар. наук.-пр. конф.*, Одеса, 26–27 жовтня 2017 р., Т. 1, Одеса: ОНАЗ, С. 106-108.

[6]. Офіційний сайт кіберполіції України: про підрозділ. [Електронний ресурс]. Режим доступу: https:// cyberpolice.gov.ua/contacts/.

[7]. Про основні засади забезпечення кібербезпеки України: Закон України. *Урядовий кур'єр*, № 215, 2017.

[8]. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про Стратегію кібербезпеки України": Указ Президента України. *Урядовий кур'єр*, № 52, 2016.

[9]. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 28 с., 2019. [Електронний ресурс]. Режим доступу: https:// geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato.

[10]. О. Трофименко Законодавча база забезпечення кібербезпеки держави. *Кібербезпека в Україні: правові та організаційні питання: матер. II всеукр. наук.-практ. конф.*, 17 листопада 2017 р., Одеса: ОДУВС, С. 55-56.

[11]. О. Трофименко, Я. Дубовой, "Щодо правового потенціалу безпечного функціонування кіберпростору", *Кібербезпека в Україні: правові та організаційні питання: матер. III всеукраїнської наук.-практ. конф.*, 30 листопада 2018 р., Одеса: ОДУВС, С. 5-7.

[12]. О. Трофименко, "Моніторинг стану кібербезпеки в Україні", *Правове життя сучасної України: матер. міжнар. наук.-практ. конф.*, 17 травня 2019 р., Т. 1, Одеса: Видавничий дім «Гельветика», С. 642-646, 2019.

[13]. У Держспецзв'язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. [Електронний ресурс]. Режим доступу: http:// www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576.

[14]. Функції захисту персональних даних покладено на уповноваженого. [Електронний ресурс]. Режим доступу: http:// www.ombudsman.gov.ua/ ua/ page/ zpd/.

[15]. R. Moody, "Which countries have the worst (and best) cybersecurity?" [Електронний ресурс]. Режим доступу: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

[16]. National Strategies. [Електронний ресурс]. Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

[17]. Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017), United Nations. [Електронний ресурс]. Режим доступу: https://www.un.org/press/en/2017/sc12714.doc.htm.

CYBERSECURITY OF UKRAINE: ANALYSIS OF THE CURRENT SITUATION

Given the rapid growth of cyber-risks and cyber-threats, monitoring the current state of our country's cybersecurity, highlighting the main problems of building a national cyber defense system and identifying ways to solve them are important. It requires both an analysis of steps already implemented to protect computer and telecommunication networks against cyberattacks, as well as the identification of the necessary steps to create conditions for the safe functioning of cyberspace. The study shows significant political, economic and social efforts to enhance cyber-resilience that the state is making to develop national cybersecurity capabilities. Effective cybersecurity needs to be addressed comprehensively and requires coordinated actions at national, regional, and international levels to prevent, prepare for, respond to and recover from incidents by government, the private sector, and civil society. Political, scientific, technical, organizational and educational issues are identified. It is necessary to solve them in the framework of complex counteraction to cyber threats in order to respond quickly to the dynamic changes occurring in cyberspace. More efforts should be made to establish public-private partnerships, to develop and implement a mechanism for the exchange of information between public authorities, the private sector and citizens regarding threats to the critical information infrastructure. Ukraine should step up its participation in the organization of joint international cyber-capacity building projects in order to coordinate actions and find new ways in strengthening cybersecurity and protection of critical information infrastructures in response to new trends in the global movement towards the digital economy and information society.

Keywords: cybersecurity, cyberattacks, cyberincidents, cybercrime, information security, cybersecurity strategy.

КИБЕРБЕЗОПАСНОСТЬ УКРАИНЫ: УГРОЗЫ, ВЫЗОВЫ, РЕШЕНИЯ

В условиях стремительного роста киберрисков и киберугроз важно мониторить состояние кибербезопасности нашей страны, выявление проблем национальной системы киберзащиты и определение направлений их решения. Для этого необходим как анализ уже реализованных мероприятий в сфере защиты компьютерных и телекоммуникационных сетей от кибератак, так и определение необходимых для реализации мероприятий по созданию условий для безопасного функционирования киберпространства. В статье проанализирован комплекс мер для решения стратегических, правовых, политических, технических и организационных вопросов для безопасного функционирования киберпространства. Выяснено, что эффективное обеспечение кибербезопасности требует комплексного решения и скоординированных действий на национальном, региональном и международном уровнях для предотвращения инцидентов со стороны органов власти, частного сектора и гражданского общества.

Ключевые слова: кибербезопасность, кибератака, киберинциденты, киберугрозы, информационная безопасность, стратегия кибербезопасности.

Трофименко Олена Григорівна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».
E-mail: egt@ukr.net.
Orcid ID: 0000-0001-7626-0886.
Трофименко Елена Григорьевна, кандидат технических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Trofymenko Olena, Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".

Прокоп Юлія Віталіївна, кандидат історичних наук, старший викладач кафедри інформаційних технологій Одеської національної академії зв'язку ім. О.С. Попова.
E-mail: yulia13.prokop@gmail.com.
Orcid ID: 0000-0002-6608-3668.
Прокоп Юлия Витальевна, кандидат исторических наук, старший преподаватель кафедры информационных технологий Одесской национальной академии связи им. А.С. Попова.
Prokop Yuliya, Candidate of Historical Sciences, Senior lecturer at the Department of Information Technology of the O.S. Popov Odessa National Academy of Telecommunications.

Логінова Наталія Іванівна, кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»
E-mail: loginova@onua.edu.ua.
Orcid ID: 0000-0002-9475-6188.
Логинова Наталья Ивановна, кандидат педагогических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Loginova Nataliia, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".

Задерейко Олександр Владиславович, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».
E-mail: zadereyko@onua.edu.ua.
Orcid ID: 0000-0003-0497-9861.
Задерейко Александр Владиславович, кандидат технических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Zadereyko Olexander, Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".