ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 351.862.48
DOI 10.36030/2310-2837-1(100)-2021-30-39

КІБЕРБЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ

О. Ж. Скибун,
Адміністрація Державної служби спеціального зв'язку та захисту інформації України

У статті розглянуто необхідність посилення заходів з кібербезпеки систем електронних комунікацій та інформаційно-аналітичних систем державного сектору (далі – СЕК та ІАС ДС), розвиток яких відбувається в рамках реалізації програм та проєктів «Цифрова держава», «Країна в смартфоні». За приклад взяті мережі та системи електронних комунікацій та інформаційно-аналітичні системи Міністерства внутрішніх справ України, Міністерства охорони здоров'я України, служб екстреного виклику (101, 102, 103, 112), Порталу Дія тощо. Відзначено, що серйозним поштовхом для прискорення процесів цифровізації, інформатизації та віртуалізації державно-управлінських функцій і взаємовідносин між громадянином та державою (перехід від режиму офлайн-комунікації громадян з державою та бізнесом до режиму онлайн) стали карантинні заходи через поширення пандемії коронавірусу SARS-CoV-2. Значне збільшення кількості СЕК та ІАС ДС, а також споживачів послуг, які надаються цими системами, стало передумовою підвищення рівня кіберзагроз, оскільки зросла кількість акторів та аудиторія системи інформаційної безпеки. Констатовано, що людський фактор (а саме рівень цифрової та кібернетичної компетентностей) впливає як на самі кіберзаходи, так і на участь у кіберінцидентах. Запропоновано для посилення ефективності здійснення кіберзахисту своєчасно та в повному обсязі реалізовувати всі завдання в рамках «Цифрової держави», «Країні в смартфоні», Цифрової адженди та стратегії «Україна 2030Е – Країна з розвинутою цифровою економікою». Обґрунтовано необхідність побудови й забезпечення функціонування загальнодержавної системи інформаційної безпеки України.
Ключові слова: кібербезпека; кіберзагрози; системи електронних комунікацій; інформаційно-аналітичні системи; цифровізація; інформатизація; стійкість та сталість функціонування комунікаційних мереж; інформаційна безпека.

CYBERSECURITY OF ELECTRONIC COMMUNICATIONS SYSTEMS OF STATE AUTHORITIES OF UKRAINE

O. Zh. Skybun,
State Service of Special Communications and Information Protection of Ukraine

The article considers the need to strengthen measures for cybersecurity of electronic communications systems and information-analytical systems of the public sector, the development of which takes place in the implementation of programs and projects «Digital State», «Country in a smartphone». Examples are electronic communication networks and systems and information-analytical systems of the Ministry of Internal Affairs, the Ministry of Health, emergency services (101, 102, 103, 112), the Action Portal, etc. It was noted that a serious impetus to accelerate the process of digitization, informatization, and virtualization of public administration functions and the relationship between citizen and state (transition from offline communication between citizens and business and online) were quarantine measures due to the spread of the SARS-CoV pandemic 2. A significant increase in the number of systems and information-analytical systems of the public sector, as well as consumers of services provided by the systems, was a prerequisite for increasing the level of cyber threats, as the number of actors and audience of the information security system increased. It was noted that the human factor (namely the level of digital and cyber competence) affects both the cyber activities themselves and participation in cyber incidents. Proposed to increase the effectiveness of cyber defense timely and fully implement all tasks within the framework of «Digital State», «Country in a smartphone», Digital Agenda and strategy «Ukraine 2030E – a country with a developed digital economy». The necessity of building and ensuring the functioning of the national information security system of Ukraine was also substantiated.
Keywords: cybersecurity; cyberthreats; electronic communication systems; information-analytical systems; digitalization; informatization; stability and sustainability of communication networks; information security.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Подальша цифровізація інформації, інформаційних та комунікативних процесів виступають каталізатором розвитку інформаційно-комунікаційних технологій, електронних комунікацій і інформаційної інфраструктури в цілому. При цьому відбувається подальша цифровізація сфер суспільства, суспільних, виробничих та економічних процесів, коли е-економіка швидко інтегрується в традиційну економіку, інформаційна інфраструктура набуває

ознак критичної інфраструктури та інтегрується в критичну інфраструктуру (далі – КІ) і все частіше стає головним елементом функціонування традиційної інфраструктури. Тому виробничі, технологічні процеси та процеси управління все більше будуються на базі складових, таких як: штучний інтелект, інтернет речей, бази даних, а комунікаційною основою виступають електронні комунікації, інтернет-мережа, телекомунікаційні послуги та послуги на базі телекомунікацій. Прикладами цього виступають цілі сфери та окремі об'єкти інфраструктури, енергетики, медицини, освіти, фінансові установи, підприємства роздрібної торгівлі (гіпермаркети, супермаркети), оператори з доставки (Glovo, Rocket тощо) та інші. Адже «сучасний етап промислової революції пов'язаний із розвитком комунікативних інтернет-технологій, які суттєво змінили технологію бізнес-процесів і отримали назву «цифровізації», коли «основою Четвертої промислової революції та третьої хвилі глобалізації стала цифрова економіка», а «особливістю цифрової економіки є її зв'язок із т. зв. економікою на вимогу (on-demand economy), яка передбачає не продаж товарів і послуг, а отримання доступу до них саме в той момент, коли це потрібно» (Цифрова економіка, 2020). Особливого значення набуває впровадження результатів цифрової та промислової революцій у сфери КІ, в рамках чого КІ стає в цілому досить «чутливою» до кіберзагроз. При цьому необхідно враховувати, що широке впровадження новітніх цифрових технологій у повсякденне життя пересічних громадян створює широке поле для можливостей впливу на процеси й відносини ззовні, адже така поширеність розмиває рівень відповідальності та можливості щодо захисту. Особливо це набуло поширення за лавиноподібного збільшення рівня включення простих громадян у процеси інформатизації як на рівні взаємовідносин із державою, так і на суспільному рівні.

Прикладом взаємовідносин із системами електронних комунікацій органів влади всіх рівнів є надання різного виду адміністративних послуг та послуг доступу до відкритих даних, різноманітних баз даних у режимі онлайн. Крім того, почали широко впроваджуватися програми та проєкти в рамках «е-суспільство» та «е-влада». Вказані тенденції стали поширеним трендом у високорозвинених країнах та країнах, які ставлять за мету стрімкий перехід від традиційних до постінформаційного етапу цивілізаційного розвитку. Такі широкі можливості перед усіма країнами, незалежно від рівня їх розвитку, відкриваються завдяки цифровим технологіям, глобалізації та інтеграції.

Водночас необхідно зазначити, що «вихід з існуючої турбулентності на траєкторію стійкого зростання супроводжуватиметься шоками для країн, що не створили вчасно технологічні, економічні та політичні передумови нового підйому», адже «у нових умовах та країна отримає переваги в результаті технологічних і цифрових інновацій, в якій розвиваються, взаємодіють, удосконалюються і зростають усі складові економіки» (Цифрова економіка, 2020). Головною відмінністю сучасності є те, що строки змін та трансформацій стають все коротшими і починають вираховуватися десятиліттями, тоді як традиційні етапи розвитку продовжувалися близько тисячі років (землеробство), кілька століть (виробництво), коли «послідовна еволюція технологій у світі створює нові виробничі інструменти і можливості для різних економічних агентів», а «нові економічні уклади виникають унаслідок т. зв. «промислових революцій»» (Цифрова економіка, 2020).

Слід звернути увагу, що сьогодні до «технологічного», «економічного» та «соціального» факторів впливу на суспільний розвиток долучається і новий, спровокований гострою респіраторною хворобою COVID-19, викликаною коронавірусом SARS-CoV-2, а саме – пандемія, яка набула світового масштабу, поширившись практично на всі країни світу. У рамках боротьби з новою пандемією багато країн уводить локдауни, забороняють офлайн-роботу багатьох закладів та установ як сфери обслуговування, так і фінансів, освіти, культури, органів влади всіх рівнів тощо. Такий швидкий і стрімкий перехід із фізичних процесів взаємовідносин та роботи у віртуальний простір ще більше впливає на рівень цифровізації взаємовідносин на рівні громадянин–суспільство–влада. У таких умовах «перехід до віддаленої роботи потребував технологічних рішень – розвитку IT-інфраструктури, системи безпеки, комунікацій, електронної постановки завдань і відстеження їх виконання. І разом з тим виникла необхідність навчання персоналу тому, як усе це використовувати та адаптуватися до змін» (Цифрова економіка, 2020).

Вказане приводить до зростання кількості населення/споживачів, які включаються у взаємовідносини в онлайн-режимі. З одного боку, це можна тільки вітати, але разом із підвищенням рівня цифровізації (діджиталізації) зростає рівень загроз та протиправних дій на кібернетичному (віртуальному) рівні. Так, «згідно зі звітом Всесвітнього економічного форуму, кібератаки

належать до п'ятірки головних небезпек, що загрожують людству, поряд із природними катастрофами і зміною клімату», а при цьому «кіберзлочинність зросла в десятки разів», коли «за приблизними оцінками, щорічний збиток світовому бізнесу від кібератак становить до 600 млрд дол. США)» (Цифрова економіка, 2020). У свою чергу, від кіберзлочинів потерпає не тільки бізнес, а й населення разом із державою в умовах поширення рівня взаємодії у віртуальному просторі в рамках поширення впровадження програм та проєктів з питань «е-суспільства», «е-влади» та інформатизації, швидкість поширення та площа охоплення яких стрімко зросла завдяки пандемії. В. Фісун наголошує на тому, що «володільцем найбільшої кількості персональних даних є держава, тому саме до неї висуваються найсуворіші вимоги щодо їх збереження та уникнення поширення у випадках, коли це не передбачається згодою особи» (Фісун). Ось чому питання кібербезпеки все більше виходить на рівень національної безпеки і потребує посиленої уваги для запобігання кіберзагрозам та їх знешкодження.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми впливу кіберзагроз на взаємовідносини між суспільством і владою в рамках подальшої цифровізації та інформатизації соціально-державного діалогу та державно-управлінських відносин показав значну увагу з боку науковців, серед яких можна відзначити таких як: Є. Аушев, О. Берназюк, Р. Дзюбаненко, О. Додонов, Ю. Жидовленко, О. Коваль, М. Кольцов, Є. Котух, М. Маюров, В. Михайлов, С. Савинов, О. Титаренко, В. Фісун, П. Цепков та ін. Однак варто відзначити, що на сьогодні залишається відкритим кіберзахист інформаційно-телекомунікаційних та інформаційно-аналітичних державних і приватних систем, а тому питання кібербезпеки систем електронних комунікацій органів державної влади набуває актуальності.

Формулювання цілей (мети) статті. Метою статті є дослідження впливу кіберзагроз на функціонування систем електронних комунікацій державних органів влади в сучасних умовах.

Виклад основного матеріалу. Поступово новітні інформаційно-телекомунікаційні технології, цифрові інформаційні та комунікативні процеси разом із програмами та проєктами інформатизації багатьох процесів державного управління, взаємовідносин із громадянами (надання адміністративних послуг, послуг з доступу до баз даних та доступу до відкритих даних, володільцем яких є держава) змінюють сутність державно-владних відносин, а також впливають на формування й реалізацію державних політик у всіх сферах суспільного життя. Положеннями Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки (далі – Цифрова адженда) визначається, що «важливими для розвитку цифрової економіки є м'які цифрові інфраструктури, які також не повинні залишатися поза увагою, зокрема інфраструктура ідентифікації та довіри, інфраструктура відкритих даних, інфраструктура інтероперабельності, інфраструктура блокчейн, інфраструктура електронних розрахунків та трансакцій, інфраструктура електронної комерції та онлайн-взаємодії суб'єктів бізнесу, інфраструктура державних послуг (електронне урядування), інфраструктура життєзабезпечення (медицина, освіта, громадська безпека, транспорт тощо), геоінформаційна інфраструктура, промислові цифрові інфраструктури» (Про схвалення Концепції, 2018). Базовою основою і транспортною артерією подальшої цифровізації та глобалізації виступають електронні комунікації (телекомунікації та/або електрозв'язок). Так, міжнародний електрозв'язок та глобальна мережа передачі даних створили сучасну конструкцію світових комунікацій, в які включені практично всі країни, незважаючи на державний устрій та форми правління. Це в остаточному підсумку дало змогу створити кіберпростір та побудувати нову віртуальну реальність.

Держава все більше включається в процеси цифровізації, інформатизації процесів взаємовідносин на рівні людина–суспільство–держава та при виконанні державно-управлінських функцій. Вказане потребує побудови й використання інформаційно-телекомунікаційних систем, а також систем електронних комунікацій, адже завдяки збільшенню рівня цифрових форматів обробления, передавання, отримання, зберігання та захисту інформації електронні комунікації (телекомунікації) виступають головною транспортною складовою сучасних процесів комунікації.

У рамках нашого дослідження розглянемо питання кібербезпеки використання систем електронних комунікацій органів державної влади України, які спрямовані на роботу з громадянами та для громадян. До таких систем комунікацій потрібно віднести функціонування служб екстреного виклику (101, 102, 103, 112 та 104), роботу гарячих ліній (державного рівня: гаряча ліня КМУ, гаряча лінія розшуку дітей, гаряча лінія міста Києва тощо), комунікаційної мережі правоохоронних органів та комунікаційної мережі охорони здоров'я, а також надання адміністра-

тивних електронних послуг в Україні, послуг з доступу до баз даних та доступу до відкритих даних. Особливість функціонування вказаних вище систем електронних комунікацій органів державної влади України (далі – СЕКОДВ) впливає на забезпечення громадян базовим рівнем безпеки, медичного забезпечення та адміністративних послуг. Розглянемо зазначене на прикладах систем електронних комунікацій Міністерства внутрішніх справ України (далі – МВС), Міністерства охорони здоров'я України (далі – МОЗ), служб екстреного виклику та Єдиного державного вебпорталу електронних послуг.

Так, «ураховуючи загальнодержавні пріоритети в реалізації проєктів взаємодії органів державної влади для об'єднання інформаційних ресурсів» було організовано функціонування «Єдиної цифрової відомчої телекомунікаційної мережі МВС» (далі – ЄЦВТМ), яка «забезпечує функціонування єдиного інтегрованого телекомунікаційного простору МВС, доставку інформації, яка циркулює в ЄЦВТМ, управління, взаємодію між підрозділами суб'єктів ЄЦВТМ, інтеграцію функціонуючих розрізнених телекомунікаційних мереж окремих суб'єктів ЄЦВТМ» та «передавання інформації, яка належить до державних інформаційних ресурсів, з метою задоволення потреб споживачів у сервісних послугах ЄЦВТМ як у звичайних умовах, так і під час особливого періоду, а також в умовах надзвичайних ситуацій чи запровадження надзвичайного стану» (Про затвердження Положення про мережу МВС, 2016). Водночас МВС було створено та введено в експлуатацію Єдину Інформаційну Систему Міністерства внутрішніх справ (далі – ЄІС МВС). Так, «функціональними підсистемами єдиної інформаційної системи МВС є: національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства; інформаційний портал Національної поліції України; Єдиний державний реєстр транспортних засобів; Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху; система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі; система екстреної допомоги населенню за єдиним телефонним номером 112; інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон; інформаційно-телекомунікаційна система прикордонного контролю Гарт-1; інші системи, реєстри та бази (банки) даних, створені суб'єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень» (Про затвердження Положення, 2018).

Що стосується питань кіберзахисту в ЄЦВТМ, то в Положенні про єдину цифрову відомчу телекомунікаційну мережу МВС є окремий розділ, який регламентує питання щодо «комплексної системи захисту інформації в ЄЦВТМ». Аналогічним чином регламентується питання кіберзахисту в ЄІС МВС, а саме «комплексні системи захисту інформації забезпечують захист інформації в підсистемах єдиної інформаційної системи МВС шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого ознайомлення з нею та/або її модифікації» (Про затвердження Положення, 2018). Крім того, значна частина сервісів, які продукуються в рамках ЄІС МВС, використовуються в різних проєктах з інформатизації, обміну даними та з доступу до відкритих даних. Вони наведені в додатку до Постанови Кабінету Міністрів України «Перелік пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ», які надаються МВС, Державною міграційною службою, Державною судовою адміністрацією, Адміністрацією Держприкордонслужби, Національною поліцією, Державною службою України з надзвичайних ситуацій, Генеральною прокуратурою.

Отже, необхідно відзначити, що стійкість та сталість функціонування як ЄЦВТМ, так і ЄІС МВС впливає на рівень якості роботи всієї правоохоронної сфери країни. Крім того, на сьогодні, за інформацією на сайті «Урядовий портал», «запущено мобільний застосунок Дія – доступ громадян до цифрових документів», у якому «доступні такі документи: цифровий паспорт громадянина України у формі ID-картки та цифровий паспорт громадянина України для виїзду за кордон (1 країна у світі); цифрове водійське посвідчення (10 країна у світі); цифрове свідоцтво про реєстрацію транспортного засобу та обов'язковий поліс страхування на авто; цифровий студентський квиток; можливість отримання нотифікацій» (Розвиток електронних послуг). Користувачами вказаного додатка є понад «4,5 млн громадян» (Розвиток електронних послуг). Крім того, «створено та запущено Єдиний державний вебпортал електронних послуг – Портал Дія (Державні послуги онлайн)», на якому «кожен громадянин може отримати електронні послуги – доступно 33 електронні послуги) та інформацію про себе з державних електронних

інформаційних ресурсів», а саме: «єдиний державний реєстр юридичних осіб, фізичних осіб–підприємців та громадських формувань; державний реєстр речових прав на нерухоме майно; єдиний державний реєстр зареєстрованих транспортних засобів та їх власників Міністерства внутрішніх справ України; державний земельний кадастр; державний реєстр обтяжень рухомого майна» (Розвиток електронних послуг). Також «запроваджено е-систему у сфері будівництва, що має на меті максимальну автоматизацію та прозорість усіх процесів у галузі: запроваджено новий сучасний та безпечний будівельний реєстр і публічний портал з повним доступом до всіх даних, у т. ч. на мапі; надання автоматичних послуг (без чиновника), що повністю нівелює будь-які корупційні ризики; створення та ведення всіх документів в електронній формі одразу в системі (містобудівні умови, будівельний паспорт) (Розвиток електронних послуг).

Таким чином, з упевненістю можна говорити про те, що рівень надання електронних адміністративних послуг та різних цифрових сервісів набирає оберти, широко входить у повсякденне буття і стає звичним явищем для пересічних громадян. О. Берназюк, досліджуючи питання «впровадження адміністративних електронних послуг в Україні», відзначає, що «переведення адміністративних послуг в електронну форму вирішує два завдання: спрощує процес їх отримання і ліквідує корупційні схеми, пов'язані з їх наданням» (Берназюк, 2019). Це створює більш сприятливі умови для формування іміджу «соціально-орієнтованої держави», покращує інвестиційний клімат та ведення бізнесу в Україні.

Наступним важливим суспільним продуктом є побудова електронної системи охорони здоров'я та створення мінімального життєздатного продукту в рамках електронної системи – eHealth в рамках медичної реформи в Україні, яка продовжується сьогодні. Як зазначається, «система eHealth структурно складається з центрального і периферійного рівнів, які в ідеалі повинні розвиватися синхронно», де «Центральний компонент системи eHealth – це центральна база даних державної системи електронної охорони здоров'я, яка накопичує дані в центральному сховищі. Доступ до цих даних є в Міністерства охорони здоров'я, Національної служби здоров'я України і постачальників медичних послуг, підключених до системи. Інформація в eHealth надходить з периферійного рівня – медичних установ, які передають дані через медичні інформаційні системи (далі – МІС)», а «МІС для медичного закладу – це інструмент, призначений не тільки для передавання даних в Центральну базу даних eHealth, а й також для вирішення локальних питань управління медичним закладом» (Що таке eHealth).

У цілому електронну систему eHealth можна охарактеризувати як «сукупність інформаційних сервісів для лікарів, пацієнтів і державних органів системи охорони здоров'я, призначених для систематизації всієї медичної інформації», де «для медустанов – це автоматизовані інструменти управління робочими процесами – медичні інформаційні системи», «для пацієнтів – зручні вебсервіси та мобільні додатки для дистанційного запису до лікаря, доступу до власної медичної інформації та онлайн-консультацій», а «для держави медична програма eHealth – це джерело даних про роботу всієї системи охорони здоров'я, які є базою для ухвалення стратегічних управлінських рішень» (Що таке eHealth). Зважаючи на вищезазначене, можна говорити про високу відповідальність щодо організації безпеки зберігання медичних та персональних даних практично про всіх громадян країни. За таких обставин питання кіберзахисту електронної системи eHealth та МІС повинні забезпечуватись на державному рівні.

Далі ми звернемося до такого важливого призначення СЕКОДВ, як основа побудови служби екстреної допомоги населенню за номерами 101, 102, 103, 104 та 112 (далі – СЕДН). Положеннями Цифрової адженди зазначається, що «використання цифрових технологій повинно запровадити новий рівень координації діяльності оперативних, чергових, диспетчерських та муніципальних служб, відповідальних за громадську безпеку та повсякденну життєдіяльність місцевих громад, а також запровадити механізми швидкого реагування відповідних служб з метою усунення наслідків правопорушень та надзвичайних ситуацій» (Про схвалення Концепції, 2018). На сьогодні «система допомоги населенню побудована на значній кількості відокремлених відомчих служб екстреної допомоги населенню (протипожежної та рятувальної справи ДСНС – «101», громадської безпеки та охорони правопорядку Нацполіція – «102», швидка медична допомога – «103», служба газу – «104», інші аварійні служби водопровідних, каналізаційних, теплових мереж, електромереж тощо), диспетчерські служби яких мають різні телефонні номери виклику, отримують інформацію та реагують тільки на ті надзвичайні події, що належать до їхньої компетенції» (Концептуальні рішення, 2010). Такий

підхід криє в собі додаткові ризики із кібербезпеки через збільшення кількості об'єктів критичної інфраструктури та акторів, які працюють із цими СЕКОДВ, адже знижується сталість та стійкість паралельного функціонування кількох СЕКОДВ. При цьому, крім систем електронних комунікацій, функціонують побудовані на їх основі відповідні платформи (інформаційно-аналітичні системи, центри обробки даних тощо), які формують окремі системи допомоги населенню (101, 102, 103, 104 тощо). Вихід із цього становища вбачається у побудові системи екстреної допомоги населенню за єдиним телефонним номером «112» (далі – Система 112), яка функціонуватиме на єдиній системі електронних комунікацій «112» та матиме єдину інформаційну систему «112».

Вказане йде у мейнстримі зі світовим досвідом впровадження систем 112 та 911, а тому створення національної Системи 112 у контексті «побудови єдиної ефективної системи реагування на загрози життю та/або здоров'ю людини, протиправні дії, надзвичайні ситуації й інші надзвичайні події, шляхом впровадження механізму координації дій усіх служб екстреної допомоги населенню на основі комплексного розв'язання проблеми – переходу від практики виконання своїх функцій за відомчою підпорядкованістю до комплексного вирішення завдань, що виникають при надзвичайних подіях з урахуванням вимог стандартів Європейського Союзу» (Концептуальні рішення, 2010) дасть змогу здійснювати комплексний підхід до питань кіберзахисту Системи 112 у цілому. Водночас необхідно враховувати, що в подальшому «надання екстреної допомоги населенню можливо завдяки удосконаленню наявних у складі територіальних органів ДСНС України оперативно-координаційних центрів, оперативно-диспетчерських служб органів державної влади та органів місцевого самоврядування з їх інтеграцією в системи 112, що забезпечують взаємодію державних та муніципальних підрозділів екстреної допомоги населенню» (Михайлов, 2015). Це, у свою чергу, збільшує кількість акторів, задіяних у системі кіберзахисту Системи 112, а також інфраструктурних, технологічних, організаційних та нормативних ресурсів.

Зважаючи на вищезазначене, огляд СЕКОДВ МВС та МОЗ (а разом з ними інші органи влади та установи, що спільно формують ЄЦВТМ, ЄІС МВС, eHealth, МІС, Дія, СЕДН, Система 112 тощо) дає нам певне уявлення про обсяги інформації, які щодня обробляються, передаються, отримуються, зберігаються та потребують захисту на всіх етапах проходження інформації. А тому «забезпечення надійної, захищеної інфраструктури, що адаптується під специфіку організації/підприємства/задачі, спроможна реалізувати та підтримати технологічні процеси обробки та збереження інформації в електронному вигляді», а також «створення та постійна підтримка такої інфраструктури силами окремо взятої організації або підприємства є трудомістким та коштовним процесом», що «особливо актуальне для державних органів, установ та підприємств, адже вони повинні забезпечувати безперебійну та захищену обробку державних інформаційних ресурсів та/або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також здійснювати розвиток, модернізацію і супроводження таких інформаційних систем в умовах обмежених часових рамок та бюджету» (Кейс, 2020). Вказане корелюється з думкою багатьох експертів з питань кіберзахисту, які визначають два підходи до інформаційної безпеки, а саме індивідуальний, «коли кожна компанія, кожен державний інститут займається побудовою власної системи інформаційної безпеки», недоліками якого є «висока вартість і неможливість відстежити всі ризики власними силами навіть для великих структур» та колективний, «пов'язаний з побудовою колективних систем інформаційної безпеки на рівні галузей і відомств» (Савинов, 2019). Адже «забезпечення системи захисту даних та регулювання конфіденційності, розробки національного плану регулювання в надзвичайних ситуаціях у кіберпросторі, управління національними кризами та забезпечення захисту критично важливої інформації» (Котух, 2020).

На наш погляд, побудова загальнодержавної системи інформаційної безпеки (далі – ЗСІБ) із запровадженням високого рівня партнерської взаємодії між державою та бізнесом у сучасних реаліях виступає найбільш вдалою та дієвою. Незважаючи на широкий спектр потрібних ресурсів, для створення та функціонування ЗСІБ необхідно виділити людський ресурс («акторів» системи інформаційної безпеки), адже тільки від рівня його комунікативних, цифрових, ІТ-, кібернетичних компетентностей та навичок залежить ефективність заходів із кіберзахисту та стійкість і сталість функціонування не тільки СЕКОДВ, а й інформаційно-аналітичних систем, побудованих на цій базі. Так, О. Титаренко, розглядаючи «формування культури кібербезпеки в органах публічного управління України», відзначає таке: «безпека та стійкість інформаційних систем стають завданнями не тільки для фахівців і груп забезпечення безпеки персоналу» і «якщо ІТ-відділ відповідає

за безпеку мережі, то запобігання вторгненням стає справою кожного», то «кібербезпека стає колективною відповідальністю і всі публічні службовці повинні нести особисту відповідальність», а «персонал повинен розуміти, що кібербезпека – це справа кожного, особливо якщо йдеться про сферу публічного управління» (Титаренко, 2018). Також важливою є наявність аналогічних компетентностей і в «аудиторії» користувачів/споживачів послуг СЕКОДВ та ЄІС державного і приватного секторів, оскільки «люди недостатньо комп'ютерно грамотні і досі не сприймають повною мірою загрози, не виконують необхідних дій з реалізації заходів кібербезпеки, не навчені культурі кібербезпеки» (Титаренко, 2018). Крім того, пересічний громадянин, на жаль, мало приділяє уваги питанням кіберзахисту власного середовища, а саме: домашній комп'ютер, ноутбук, смарттелевізор, смартфон тощо. При цьому рівень ураження «багатофункціонального кінцевого обладнання споживачів, які працюють під управлінням операційних систем» (Звіт діяльності НКРЗІ, 2020), є дуже високим. Але, незважаючи на це, їх продовжують використовувати як для комунікацій у соціальних мережах, так і для взаємовідносин із СЕКОДВ та в ЄІС державного і приватного секторів, наражаючи ці мережі та системи на кібернебезпеку. Ось чому людина та «людський фактор» часто стають відповідальними за «нештатні» кіберситуації та кіберподії на СЕКОДВ та в ЄІС державного та приватного секторів. На сьогодні «найбільшою з ключових кіберзагроз залишається соціальна інженерія – це 81 % від усього фрода (де fraud це вид шахрайства в галузі інформаційних технологій, зокрема, несанкціоновані дії і неправомірне користування ресурсами і послугами)» (Савинов, 2019). Адже штучний інтелект і машини діють за встановленим алгоритмом і не роблять ірраціональні вчинки (як людина). Можна привести досить поширені приклади, а саме: «дуже прості паролі», які до того ж можуть не змінюватися довгий час, використання «власних» накопичувачів інформації в службових пристроях, «блукання по сайтах» на службових машинах, передача прав допуску до автоматичного робочого місця та/чи інформації третіх осіб тощо. Тому «захист кіберпростору вимагає ефективних і дієвих заходів, які можуть бути реалізовані шляхом прийняття найкращих практик та стандартизації поведінки» за умов наявності «людського, організаційного, інфраструктурного, технологічного, нормативного» вимірів кібербезпеки (Котух, 2020). А тому найбільш ефективним є «не просто протидія кібератакам, а розробка системи, яка дасть змогу прогнозувати виникнення нових загроз» (Савинов, 2019). За таких обставин «держава має докласти всіх зусиль, щоб суспільство знало про наявні ризики, а також надати консультаційну та технологічну підтримку в упровадженні та використанні захищених інформаційно-комунікаційних систем, інфраструктур, платформ тощо» (Україна 2030Е). Передусім необхідно провести «початковий аудит на об'єктах критичної інфраструктури з точки зору оцінювання техногенних ризиків та дотримання міжнародних безпекових стандартів» (Стратегія розвитку, 2019), які є в СЕКОДВ та в ЄІС державного та приватного секторів.

Так, у рамках стратегії «Україна 2030Е – Країна з розвинутою цифровою економікою» визначаються критичні завдання для Національної системи кібербезпеки України, а саме «скласти та затвердити перелік систем критичної інфраструктури (СКІ); провести аудит стану кібербезпеки СКІ з наданням відповідних рекомендацій щодо збільшення рівня захищеності та реагування на інциденти; створити центральні (ДССЗЗІ та СБУ вже створені) та галузеві центри запобігання кіберінцидентам та реагування на них (SOC, CERT) (згідно з європейською практикою транспортний, енергетичний, фінансовий, телекомунікаційний, медичний, продовольчо-забезпечувальний рівні); розробити галузеві стандарти (настанови, інструкції) з кібербезпеки об'єктів СКІ та визначити механізми перевірки їх дотримання й оцінки виконання; розробити методику та заходи щодо проведення лабораторних та польових кібернавчань для спеціалістів і керівників СКІ та державних установ» (Україна 2030Е, 2020). Зазначені заходи доцільно застосовувати для СЕКОДВ та в ЄІС державного та приватного секторів. Водночас необхідно додати до вказаного ще одне завдання, яке стосується розвитку комунікативних, цифрових, ІТ-, кібернетичних компетенцій та навичок громадян, а також формування культури кібербезпеки в акторів у кіберпросторі та в аудиторії системи кібернетичної безпеки для СЕКОДВ та в ЄІС державного та приватного секторів.

Висновки та перспективи подальших досліджень. Підсумовуючи дослідження питань кібербезпеки систем електронних комунікацій органів державної влади, необхідно відзначити таке. Стрімке зростання присутності держави в цифровому (віртуальному просторі) обумовлюється сучасними тенденціями впровадження програм та проєктів з інформатизації в рамках «е-суспільство» та «е-влада». Означене зумовлене побудовою нових сучасних комунікаційних

мереж, створенням інформаційно-телекомунікаційних систем (як на рівні окремих відомств, установ, так і на загальнодержавному рівні). Додатковим поштовхом до прискорення цифровізації державно-управлінських функцій та взаємовідносин між громадянином і державою стали наслідки поширення пандемії коронавірусу SARS-CoV-2 на світовому рівні, коли під час карантинних заходів почався перехід від режиму офлайн-комунікації громадян з державою та бізнесом до режиму онлайн. Широке впровадження соціально-державних відносин у віртуальному просторі спровокувало зростання рівня кіберзагроз та кіберзлочинів у СЕКОДВ та в ЄІС державного та приватного секторів. На сьогодні одним із головних факторів, який вплинув на збільшення рівня кіберзагроз та кіберзлочинів, є людський фактор. Передусім багаторазово збільшилась кількість громадян, які почали використовувати цифрові технології та отримувати онлайн-послуги і все більше часу проводити у віртуальному просторі. При цьому, як виявилося, рівень комунікативних, цифрових, ІТ-, кібернетичних компетентностей та грамотності щодо убезпечення себе від кіберзагроз є вкрай низьким. І це стосується як акторів, так і аудиторії СІБ. Також певна кількість акторів та аудиторії СІБ упевнені, що заходами з кіберзахисту повинні займатися лише представники відповідних підрозділів. Зважаючи на вищевказане, необхідно відзначити, що для збільшення ефективності здійснення кіберзахисту необхідно реалізовувати своєчасно та в повному обсязі всі завдання в рамках «Цифрової держави», «Країни в смартфоні», «Цифрової адженди, стратегії «Україна 2030Е – Країна з розвинутою цифровою економікою». Результатом такої роботи повинна стати побудована загальнодержавна система інформаційної безпеки України.

Подальше зростання присутності держави у віртуальному просторі та збільшення взаємовідносин між суспільством і владою в режимі онлайн (надання адміністративних електронних послуг, надання послуг з доступу до відкритих даних та баз даних, доступу до екстрених служб, зберігання персональних даних громадян в СЕКОДВ та в ЄІС) створює передумови до активізації кіберзлочинів та збільшення кіберзагроз, що потребує належного реагування, а для цього необхідно проводити відповідні розвідки.

Список використаних джерел

Берназюк О. Адміністративні електронні послуги: поняття та умови впровадження в Україні. *Підприємництво, господарство і право. Інформаційне право.* 5/2019. С. 196–199.

Державні послуги онлайн. URL: https://diia.gov.ua/ (дата звернення: 26.03.2021).

Концептуальні рішення створення автоматизованої системи екстреної допомоги населенню за єдиним телефонним номером «112» / О. Г. Додонов та ін. *Реєстрація, зберігання і обробка даних.* 2010. Т. 12. № 2. С. 165–180.

Звіт про роботу Національної комісії, що здійснює регулювання у сфері зв'язку та інформатизації за 2019 рік. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=34&id=9088&language=uk (дата звернення: 27.03.2021).

Кейс. Досвід «Українського державного центру міжнародної освіти». 2020. URL: https://ucloud.ua/kejs_kszi/ (дата звернення: 28.03.2021).

Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. *Лабораторія законодавчих ініціатив.* 2017. Груд. 28 с.

Котух Є. В. Формування систем кібербезпеки в органах публічної влади. *Державне управління: удосконалення та розвиток.* 2020. № 3. URL: http://www.dy.nayka.com.ua/?op=1&z=1596 (дата звернення: 29.03.2021). DOI: 10.32702/2307-2156-2020.3.30

Михайлов В. М. Організація взаємодії державних і муніципальних підрозділів екстреної допомоги населенню в Системі 112. *Державне управління: удоско-*

References

Bernazyuk, O. (2019). Administraty`vni elektronni poslugy`: ponyattya ta umovy` vprovadzhennya v Ukrayini. *Pidpry`yemny`cztvo, gospodarstvo i pravo. Informacijne pravo.* 5/2019. P. 196–199 [in Ukrainian].

Derzhavni poslugy` onlajn. Retrieved from: https://diia.gov.ua/ (accesed: 26 March 2021).

Dodonov, O. G., Koval`, O. V., Dzyubanenko, R. I., Cepkov, P. A., Zhy`dovlenko, Yu. O., Mayurov, M. O. (2010). Konceptual`ni rishennya stvorennya avtomaty`zovanoyi sy`stemy` ekstrenoyi dopomogy` naselennyu za yedy`ny`m telefonny`m nomerom «112». Reyestraciya, zberigannya i obrobka dany`x Vol. 12. Is. 2. P. 165–180 [in Ukrainian].

Zvit pro robotu Nacional`noyi komisiyi, shho zdijsnyuye regulyuvannya u sferi zv'yazku ta informaty`zaciyi za 2019 rik. Retrieved from: https://nkrzi.gov.ua/index.php?r=site/index&pg=34&id=9088&language=uk (accesed: 27 March 2021).

Kejs. Dosvid «Ukrayins`kogo derzhavnogo centru mizhnarodnoyi osvity`» (2020). Retrieved from: https://ucloud.ua/kejs_kszi/ (accesed: 28 March 2021).

Kol`czov, M., Aushev, Ye. (2017). Propozy`cii do polity`ky` shhodo reformuvannya sfery` kiberbezpeky` v Ukrayini. *Laboratoriya zakonodavchy`x iniciaty`v.* Gruden`. 28 p. [in Ukrainian].

Kotux, Ye. V. (2020). Formuvannya sy`stem kiberbezpeky` v organax publichnoyi vlady. *Derzhavne upravlinnya: udoskonalennya ta rozvytok.* Is. 3. Retrieved from: http://www.dy.nayka.com.ua/?op=1&z=1596 (accesed: 29 March 2021).

налення та розвиток. 2015. № 4. URL: http://www.dy.nayka.com.ua/?op=1&z=837 (дата звернення: 29.03.2021).

Про затвердження Положення про Єдину Інформаційну Систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Каб. Міністрів України від 14.11.2018 № 1024. *База даних «Законодавство України»* / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF (дата звернення: 30.03.2021).

Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС : наказ Міністерства внутрішніх справ України від 04.07.2016 № 596, зареєстровано в М-ві юстиції України 28.07.2016 № 1055/29185. URL: http://tranzit.ltd.ua/nakaz/ (дата звернення: 29.03.2021).

Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Каб. Міністрів України від 17.01.2018 № 67-р. *Уряд. кур'єр.* 2018. 11 трав. № 88.

Розвиток електронних послуг. *Уряд. портал.* URL: https://www.kmu.gov.ua/diyalnist/reformi/efektivne-vryaduvannya/rozvitok-elektronnih-poslug (дата звернення: 25.03.2021).

Савинов С. Кибербезопасность: барьер против новых «воинов тьмы». *IBS.* 2019. 21 мая. URL: https://www.ibs.ru/media/media/kiberbezopasnost-barer-protiv-novykh-voinov-tmy. (дата звернення: 24.03.2021).

Стратегія розвитку «Індустрія 4.0» (2019). URL: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi44ozt3-7vAhVMtIsKHTLuBBgQFjABegQIBxAD&url=https%3A%2F%2Fmautic.appau.org.ua%2Fasset%2F42%3Astrategia-rozvitku-4-0-v3pdf&usg=AOvVaw1jnBljb5lvF8c59iM_aS4m (дата звернення: 30.03.2021).

Титаренко О. Формування культури кібербезпеки в органах публічного управління України. 2018. URL: http://www.dridu.dp.ua/zbirnik/2018-01(19)/12.pdf (дата звернення: 25.03.2021).

Україна 2030Е – Країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення: 26.03.2021).

Фісун В. Проблеми захисту персональних даних: досвід України та інших країн. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html (дата звернення: 25.03.2021).

Цифрова економіка: тренди, ризики та соціальні детермінанти. Київ : Центр Разумкова, 2020. 274 с.

Що таке eHealth і як підключитися до системи. URL: https://emci.ua/iak-pidkliuchytysia-do-ehealth/ (дата звернення: 25.03.2021).

My`xajlov, V. M. (2015). Organizaciya vzayemodiyi derzhavny`x i municy`pal`ny`x pidrozdiliv ekstrenoyi dopomogy` naselennyu v Sy`stemi 112. *Derzhavne upravlinnya: udoskonalennya ta rozvy`tok.* Is. 4. Retrieved from: http://www.dy.nayka.com.ua/?op=1&z=837 (accesed: 29 March 2021) [in Ukrainian].

Postanova Uabinetu Ministriv Ukrayiny` (2018). Pro zatverdzhennya Polozhennya pro Yedy`nu Informacijnu Sy`stemu Ministerstva vnutrishnix sprav ta pereliku yiyi priory`tetny`x informacijny`x resursiv : vid 14.11.2018 # 1024. *Baza dany`x «Zakonodavstvo Ukrayiny`»/ Verxovna Rada Ukrayiny.*

Nakaz Ministerstva vnutrishnix sprav Ukrayiny` (2016). Pro zatverdzhennya Polozhennya pro yedy`nu cy`frovu vidomchu telekomunikacijnu merezhu MVS : vid 04.07.2016 # 596, Zareyestrovano v Ministerstvi yusty`ciyi Ukrayiny` 28 ly`pnya 2016 r. za # 1055/29185. Retrieved from: http://tranzit.ltd.ua/nakaz/ (accesed: 26 March 2021).

Rozporiadzhennia Uabinetu Ministriv Ukrayiny` (2018). Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii vid 17 sichnia 2018 r. № 67-r. *Uriadovyi kurier* vid 11.05.2018 № 88 [in Ukrainian].

Rozvy`tok elektronny`x poslug. *Uryadovy`j portal* (2020). Retrieved from: https://www.kmu.gov.ua/diyalnist/reformi/efektivne-vryaduvannya/rozvitok-elektronnih-poslug (accesed: 25 March 2021).

Savinov, S. Kiberbezopasnost: barer protiv novyih «voinov tmyi» (2019). Retrieved from: https://www. ibs.ru/media/media/kiberbezopasnost-barer-protiv-novykh-voinov-tmy (accesed: 24 March 2021).

Strategiya rozvy`tku «Industriya 4.0» (2019). URL: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi44ozt3-7vAhVMtIsKHTLuBBgQFjABegQIBxAD&url=https%3A%2F%2Fmautic.appau.org.ua%2Fasset%2F42%3Astrategia-rozvitku-4-0-v3pdf&usg=AOvVaw1jnBljb5lvF8c59iM_aS4m (accesed: 30 March 2021).

Ty`tarenko, O. (2018). Formuvannya kul`tury` kiberbezpeky` v organax publichnogo upravlinnya Ukrayiny`. Retrieved from: http://www.dridu.dp.ua/zbirnik/2018-01(19)/12.pdf (accesed: 25 March 2021).

Ukrayina 2030E – Krayina z rozvy`nutoyu cy`frovoyu ekonomikoyu (2020). Retrieved from: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (accesed: 25 March 2021).

Fisun, V. (2020). Problemy` zaxy`stu personal`ny`x dany`x: dosvid Ukrayiny` ta inshy`x krayin. Retrieved from: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html (accesed: 26 March 2021).

Cy`frova ekonomika: trendy`, ry`zy`ky` ta social`ni determinanty` (2020). Kyiv, Centr Razumkova. 274 p.

Shho take eHealth i yak pidklyuchy`ty`sya do sy`stemy` (2021). Retrieved from: https://emci.ua/iak-pidkliuchytysia-do-ehealth/ (accesed: 25 March 2021).

Скибун Олександр Жоржович,
кандидат наук з державного управління, Адміністрація Державної служби спеціального зв'язку та захисту інформації,
03110, Україна, м. Київ, вул. Солом'янська, 13.

Цитування: Скибун О. Ж. Кібербезпека систем електронних комунікацій органів державної влади України. *Вісн. НАДУ. Серія «Державне управління»*. 2021. № 1 (100). С. 30–39.

Стаття надійшла: 25.02.2021

Схвалено до друку: 01.03.2021

Skybun, Oleksandr Zh.,
Candidate of Science in Public Administration,
13, Solomianska St., Kyiv, 03110, Ukraine,
E-mail: skybun@i.ua
http://orcid.org/0000-0001-6084-5222

Citation: Skybun, O. Zh. (2021). Kiberbezpeka system elektronnykh komunikatsii orhaniv derzhavnoi vlady Ukrain [Cybersecurity of electronic communications systems of state authorities of Ukraine]. *Bulletin of the NAPA. Series «Public Administration»*. Is. 1 (100). P. 30–39 [in Ukrainian].

Article arrived: 25.02.2021

Accepted: 01.03.2021