УДК 351.862.48
DOI 10.36030/2310-2837-4(99)-2020-84-92

ВПЛИВ КІБЕРЗАГРОЗ НА ФУНКЦІОНУВАННЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ (ТЕЛЕКОМУНІКАЦІЙ) В УМОВАХ ПОБУДОВИ «ЦИФРОВОЇ ДЕРЖАВИ»

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

У статті обґрунтовано необхідність створення системи протидії кіберзагрозам на мережах електронних комунікацій (телекомунікацій) шляхом побудови чіткої вертикалі із суб'єктів, які безпосередньо у межах своєї компетенції вживають заходів щодо забезпечення кібербезпеки. Для забезпечення можливості оперативного реагування в реальному часі на загрози, що впливатимуть на стійкість функціонування національної інфраструктури, запропоновано створити Єдиний національний центр реагування на загрози, підпорядкувавши його Раді національної безпеки і оборони України, а також включити до завдань кіберзахисту заходи щодо забезпечення приватного кінцевого обладнання (багатофункціональних мобільних пристроїв) та доступу населення до електронних комунікацій (телекомунікацій) загального користування для задоволення «цифрових» потреб. Рекомендовано надання фінансових і банківських послуг та сервісів через багатофункціональні мобільні пристрої лише за умови наявного письмово контракту на надання телекомунікаційних послуг. Представлено практичні заходи щодо підвищення рівнів компетентностей (комп'ютерних, ІТ, цифрових, комунікативних, кібернетичних) населення України.
Ключові слова: кібербезпека; кіберзагрози; електронні комунікації (телекомунікації); цифровізація; інформатизація; стійкість та сталість функціонування комунікаційних мереж; нові комунікації; інформаційні процеси; телекомунікаційні послуги.

THE INFLUENCE OF CYBER THREATS ON THE FUNCTIONING OF ELECTRONIC COMMUNICATIONS (TELECOMMUNICATIONS) IN CONDITIONS OF BUILDING A «DIGITAL STATE»

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

Articles on the well-founded need to create systems to combat cyber threats on electronic communications networks (telecommunications) through the construction of a clear vertical of business entities that operate within the competence provided by cybersecurity. To be able to respond quickly to real-time threats that will affect the sustainability of the national infrastructure, it is proposed to create a single national threat response center, subordinating the National Security and Defense Council of Ukraine. It is proposed to include in the tasks of cybersecurity measures to provide private terminal equipment (multifunctional mobile devices) and public access to electronic communications (telecommunications) for general use to meet «digital» needs. It is recommended to provide financial and banking services through multifunctional mobile devices only if there is a written contract for the provision of telecommunications services. Practical measures to increase the levels of competencies (computer, IT, digital, communicative, cybernetic) of the population of Ukraine are presented.
Keywords: cybersecurity; cyberthreats; electronic communications (telecommunications); digitalization; informatization; stability and sustainability of communication networks; new communications; information processes; telecommunication services.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Подальша цифровізація та інформатизація всіх суспільних сфер та відносин створюють сучасний дискурс нових комунікацій на рівні людина-суспільство-держава. Вказане вимагає забезпечення доступу до електронних комунікацій (ЕК) (телекомунікацій) усіх верств населення на всій території країни на достатньому рівні швидкостей та обсягів отримання, оброблення, передавання, збереження та захисту інформації. При цьому якість надання ЕК повинна задовольняти постійно зростаючі вимоги до показників швидкості та обсягів передачі інформації для задоволення потреб у послугах на базі ЕК, спектр яких постійно розширюється (соціальні мережі та медіа, послуги та сервіси, доступи до баз даних, отримання цифрових державних послуг тощо). Таким чином, як зазначено в Законі України «Про телекомунікації», ЕК стають «невід'ємною частиною виробничої та соціальної інфраструктури України», задовольняючи при цьому потреби «фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах» (Закон України, 2004). Інакше кажучи, ЕК забезпечують подальшу віртуалізацію

суспільства та взаємовідносин його із бізнесом і державою, коли цифровізація інформаційних та комунікативних процесів змінює парадигму самої сутності комунікацій, формуючи нову цифрову реальність, нові цифрові взаємовідносини та цифрові комунікації. Отже, підвищення рівнів цифровізації та інформатизації і, відповідно, впливу кіберзагроз зумовлює зростання запиту на кіберзахист. Але ж, як зазначає О. Соснін, «забезпечення безпеки в інформаційно-комунікаційному середовищі стає пріоритетним напрямом науково-технічної діяльності, вимагаючи істотної уваги й зусиль з боку людини, суспільства, владних структур і юридичної науки держави» (Соснін, 2020). Вказане повною мірою характеризує сучасні реалії розвитку та широкого використання ЕК в процесах цифровізації та інформатизації усіх сфер та суспільних відносин. Адже створення сучасного нормативно-правового поля сприяє підвищенню ефективності та ролі ЕК в умовах поглибленого входження у віртуальний простір держави в рамках різних проєктів з інформатизації, де вплив кіберзагроз на стійкість та сталість функціонування ЕК зростає.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. Питанням впливу кіберзагроз на суспільство, владу, людину та суспільно-економічні, суспільно-політичні процеси і взаємини в рамках інформаційного і навіть постінформаційного суспільства значну увагу приділяли такі науковці, як: О. Баранов, В. Бурячок, С. Гнатюк, І. Жиляєв, О. Карпенко, В. Семко, О. Соснін, А. Шиян, В. Фісун та ін. Однак варто зауважити, що на сьогодні залишається відкритим питання завершення побудови системи кіберзахисту та формування центрів реагування на кіберзагрози в умовах подальшої побудови «цифрового суспільства» та «цифрової держави», а тому питання впливу кіберзагроз на функціонування електронних комунікацій (телекомунікацій) буде й надалі актуалізуватися.

Формулювання цілей (мети) статті. Метою статті є дослідження впливу кіберзагроз на функціонування електронних комунікацій (телекомунікацій) в умовах побудови «цифрової держави» та подальшого підвищення ролі віртуального простору для широких верств населення.

Виклад основного матеріалу. Постійне здешевлення вартості телекомунікаційних послуг, телекомунікаційного обладнання та кінцевих пристроїв разом із зростанням показників швидкості та обсягів передачі і зберігання даних стали передумовою надання ЕК ознак масовості та доступності для все більшої кількості громадян. Підтвердження цієї тези можна знайти у «Звіті діяльності Національної комісії, що здійснює регулювання у сфері зв'язку та інформатизації (НКРЗІ) за 2019 рік», де станом на 31 грудня 2019 р. наведено такі дані: «кількість активних ідентифікаційних телекомунікаційних карток мережі рухомого (мобільного) зв'язку становила 54 843 тис. од.», «загальна кількість активних ідентифікаційних телекомунікаційних карток мережі рухомого (мобільного) зв'язку, з яких було здійснено доступ до мережі «Інтернет», становила 34 689 тис. од.», а «кількість ліній (точок) фіксованого доступу до мережі «Інтернет» з урахуванням даних фізичних осіб-підприємців становила 7 265 тис. од. (1 173 тис. од. – в сільській місцевості)» (Звіт діяльності НКРЗІ, 2020).

Наведені цифри свідчать про те, що, незважаючи на певні проблеми із покриттям та загальним фінансово-економічним станом суспільства та економіки нашої країни, все ж відбувається «розвиток цифрових інфраструктур та цифровий розвиток пріоритетних сфер життєдіяльності, що спрямовані на подолання цифрового розриву в країні та збільшення кількості електронних послуг у таких сферах, як громадська безпека, освіта, охорона здоров'я, туризм, транспортна інфраструктура, електронна демократія, екологія та охорона навколишнього природного середовища, життєдіяльність міст, безготівкові розрахунки (e-Gov, e-Learning, e-Health, телемедицина тощо)» (Звіт діяльності НКРЗІ, 2020). Вказане відкриває можливості для широкого впровадження багатьох проєктів у рамках програм «Електронне суспільство», «Електронне врядування», «Електронна демократія», що відповідає новій національній стратегії «Держава в смартфоні», яка декларується керівництвом країни та реалізується новоутвореним Міністерством цифрової трансформації України. Це означає, що влада почала розуміти необхідність реалізації в країні сучасних проєктів із розвитку інформаційної інфраструктури, цифрового суспільства, економіки. Підвищення рівня входження у кібернетичний простір та віртуальну реальність має як позитивні, і негативні ознаки. Серед широкого спектру негативних ознак кіберзагрози займають чільне місце. Так, Законом України «Про основні засади забезпечення кібербезпеки України» вводяться такі поняття, як: «кіберзагроза», «інцидент кібербезпеки», «кібератака», «кіберзлочин (комп'ютерний злочин)», «кіберрозвідка», «кібертероризм», «кібершпигунство» (Закон України, 2017). Усвідомлення з боку суспільства, бізнесу та держави наслідків кіберзагроз

відбулося під час подій у 2016–2017 рр., коли в результаті «кібератаки в грудні 2016 р. на державні фінансові установи протягом майже трьох днів було ускладнено сплату до бюджету податків та інших платежів, заблоковано електронну систему адміністрування ПДВ, порушено роботу митниці», а «у результаті атаки вірусу NotPetya на комп'ютерні системи українських державних і комерційних установ України станом на 7 липня 2017 р. було виведено з ладу до 10 % приватних, урядових і корпоративних комп'ютерів» (Жиляєв, Семенченко, 2017).

Так, «широке використання багатофункціональних кінцевих обладнань споживачів, які працюють під управлінням операційних систем (смартфонів, планшетів)» (Звіт діяльності НКРЗІ, 2020), комп'ютерів, смартпристроїв, Інтернету речей сприяло переходу проблем кіберзахисту та кібербезпеки на побутовий рівень, коли від кіберзагроз почали потерпати не тільки державні установи, підприємства, приватні компанії, а й прості громадяни. При цьому останні опинилися найуразливішими через низький рівень захищеності перед кіберзагрозами, враховуючи відсутність дієвих інструментів захисту приватного комунікаційного обладнання, мереж та сховищ зберігання даних. До того ж приватний сектор як об'єкт захисту з боку держави і бізнесу взагалі не існує, хоча на сьогодні темпи та обсяги обміну даними між приватним та державним секторами і бізнесом постійно зростають в умовах збільшення обсягів послуг на базі телекомунікацій.

Так, Український інститут майбутнього у своїй стратегії «Україна 2030Е – Країна з розвинутою цифровою економікою» наголошує на тому, що «інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного запобігання супутнім ризикам, їх усунення та управління ними» (Україна 2030Е, 2020). Адже «рівень відповідальності влади щодо впровадження в усі сфери людської діяльності ІКТ та засобів електронно-обчислювальної техніки зростає, а інформація та інформаційні ресурси стають одним із вирішальних факторів розвитку особистості, суспільства і держави» (Соснін, 2020).

Указане вимагає від держави формування та реалізації разом із бізнесом та суспільством відповідної державної політики щодо забезпечення захистом від кіберзагроз багатофункціональних кінцевих обладнань споживачів (БКОС), які працюють під управлінням операційних систем (смартфонів, планшетів) і використовуються населенням для комунікації із державними і комерційними інформаційно-телекомунікаційними системами (ІТС), інформаційною інфраструктурою (ІІ) та критичною інфраструктурою (КІ), а також для соціальних контактів та побутових цілей. У зв'язку із цим зростає обсяг кібернетичних правопорушень та злочинів, тому актуальність питання кібербезпеки постійно підвищується. А беручи до уваги, що від рівня сталості та стійкості залежить функціонування ЕК, їх кіберзахист є важливим у системі кіберзахисту. При цьому дискурс кіберзахисту в ЕК має два напрями. Перший напрям – це безпосередній вплив кіберзагроз на стійкість та безпеку функціонування самих ЕК як складових комунікаційних мереж окремих операторів телекомунікацій, так і в системі комунікаційної мережі загального користування, другий – використання ЕК як комунікаційної-комунікативної інфраструктури для задоволення потреб населення, бізнесу та держави в новій системі комунікацій та проєктів з інформатизації.

У рамках нашого дослідження пропонуємо розглянути питання кібербезпеки та кіберзахисту таких окремих елементів, що формують «цифрове середовище», як: персональні дані, доменні імена, електронні фінансові та банківські послуги (е-фінанси та е-послуги), електронні державні послуги та сервіси, доступ громадян до баз даних в рамках проєктів «ДІЯ» та «Держава в смартфоні».

В. Фісун, досліджуючи «проблеми захисту персональних даних: досвід України та інших країн», зазначає, 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», оскільки «очевидно, що витік інформації з державних баз даних лише посилює недовіру до держави та створює відчуття незахищеності перед внутрішніми й зовнішніми загрозами» (Фісун, 2020). Прикладом може слугувати поява в нелегальному обігу різноманітних баз даних громадян, дані з яких можуть використовуватися у протиправних діях. І це незважаючи на те, що кожного разу у людини запитують дозволу на використання її персональних даних і зобов'язуються відповідно до Закону України «Про захист персональних даних» відповідними чином зберігати та обробляти їх. Адже питання захисту персональних даних стосується кожного громадянина незалежно від того, виступає він від імені приватної особи, як уповноважена державою або бізнесом особа в ін-

формаційних процесах (передавання, оброблення, отримання, зберігання).

На сьогодні досить часто громадяни дають згоду на дії з їхніми персональними даними не тільки на рівні адміністративних послуг та сервісів з боку державних установ, а й на побутовому рівні (реєстрація в магазинах, на сайтах тощо).

Слід зазначити, що аналіз положень Закону України «Про захист персональних даних» свідчить, що в основному він має декларативний характер, а контроль за його дотриманням узагалі покладено на суди та Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних (Про захист персональних даних, 2010).

Так, у ст. 24 цього Закону зазначається, що «володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, в тому числі незаконного знищення чи доступу до персональних даних» (Про захист персональних даних, 2010).

Під персональними даними розуміються «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» (Про захист персональних даних, 2010). У сучасних умовах подальшої віртуалізації та інформатизації інформаційних процесів розширюється перелік надання послуг та робіт за допомогою онлайн-ресурсів, що автоматично приводить до збільшення обсягів передачі персональних даних. На наш погляд, це може спричинити втрату самого сенсу захисту персональних даних як таких. Окремим аспектом проблеми захисту персональних даних є все, що стосується національних кордонів та правосуб'єктності «володільців, розпорядників персональних даних та третіх осіб», які вчиняють дії із персональними даними від імені громадян України. Але зважаючи на те, що віртуальний (кібер) простір не має національних кордонів і є глобальним продуктом, питання надання персональних даних іноземним суб'єктам означає збільшення ризиків щодо використання в протиправних діях.

Як показує практика, найвищий рівень кіберзлочинів та кіберзагроз сьогодні спостерігається у фінансовій та банківській сферах (використання мобільного банкінгу та різних мобільних банківських сервісів), адже незаконне використання персональних даних призводить передусім до фінансових втрат з боку пересічних громадян. На наш погляд, такий стан справ має дві сторони медалі. З одного боку, це відсутність сучасного, дієвого врегулювання на законодавчому рівні функціонування ринку надання електронних фінансових та банківських послуг (з використанням досвіду інших країн) відкриває широкі можливості для шахраїв, з другого – низький рівень цифрової-, кібер-, фінансової та правової грамотності і компетентностей самих громадян. Яскравим прикладом є використання «ідентифікаційної телекомунікаційної картки (SIM-картка, USIM-картка, R-UIM-картка тощо)» (Про порядок реєстрації, 2017), коли телекомунікаційні послуги надаються без підписання відповідного договору на надання телекомунікаційних послуг. Це означає прив'язку використання мобільного банкінгу та різних мобільних банківських сервісів до певного номеру телефону, обслуговування якого юридично не закріплено. Сьогодні широко рекламується отримання віртуальної банківської катки (банківська картка в смартфоні), при цьому в рекламі ніде не згадується, що вказані послуги будуть надаватися лише на підставі чинного договору заявника із будь-яким оператором телекомунікацій на надання телекомунікаційних послуг. Законодавчо відсутні норми заборони передавання персональних даних, отримання оплатних послуг та здійснення будь-яких фінансових і банківських операцій лише на підставі заключеного письмово договору між абонентом та оператором телекомунікацій.

Так, положеннями «Порядку реєстрації абонентів, які отримують телекомунікаційні послуги без укладення договору в письмовій формі», затвердженого Рішенням НКРЗІ від 28 листопада 2017 р. № 607, визначається право абонента «зареєструватися в оператора, провайдера телекомунікацій шляхом подання заяви про реєстрацію» (Про затвердження порядку, 2017). За таких ліберальних умов відбувається постійний обіг знеособленого номерного ресурсу там, де відбувається обіг персональних даних. Адже в разі відсутності будь-якого контролю щодо переміщення та місця проживання фізичної та/або юридичної особи номер телефону є одним із важливих елементів персональних даних, а певна його міграція відкриває широке поле для кібершахрайства та кіберзлочинів із перекладанням певних ризиків на третіх осіб, до яких перейшов у користування такий номер телефону.

Поряд з проблемою щодо захисту персональних даних існує проблема спаму, або незапрошуваних електронних повідомлень, які розповсюджуються мережею та які можна віднести до так званого «цифрового забруднення», що впливає на функціонування ЕК, зокрема на швидкість та обсяги передачі даних, а також «засмічує» сховища інформації непотрібною інформацією. Крім того, досить часто спам або незапрошувані електрон-

ні повідомлення криють у собі кіберзагрозу у вигляді шкідливого програмного продукту, який потрапляє до кінцевого обладнання споживача, впливаючи або на роботу самого пристрою, або знімаючи інформацію з нього для третіх осіб. Визначення спаму є в Законі України «Про електронні комунікації», а також прописана норма про заборону умисного масового «розсилання електронних, текстових та/або мультимедійних повідомлень без згоди (замовлення) кінцевих користувачів (спаму) на їх адреси електронної пошти або термінальне обладнання» (Про електронні, 2020). Ситуація зі спамом досить напружена з огляду на те, що на сьогодні дієвих законодавчих механізмів боротьби з ним в українському законодавстві недостатнє.

Серед кіберправопорушень на певну увагу заслуговує такий вид кіберзлочину, як кіберсквотинг, який означає здійснення махінацій та протиправних дій відносно торговельних марок та доменних імен (у віртуальному просторові). На перший погляд, питання кіберсквотингу нібито не стосуються широкого загалу, але якщо враховувати появу в глобальній мережі передачі даних двійників торгових марок та доменних імен, то відразу можна згадати про елементи кібершахрайства, адже йдеться не тільки про заволодіння персональними даними, а й номерами банківських рахунків і номерами карток для здійснення крадіжок коштів з рахунків. Крім того, такі протиправні дії створюють негативний образ офіційних торгових марок та доменних імен. Так, Д. Нікулеско, досліджуючи проблему кіберсквотингу, відзначає певний прогрес завдяки вирішенню спірних питань і питань кіберзлочинів через залучення судових інстанцій (Нікулеско, 2020), але насамперед необхідне їх більш чітке врегулювання на законодавчому рівні, оскільки захист прав на інтелектуальну власність уже після правочину через суди є досить тривалим і витратним як на національному, так і на міжнародному рівні.

У межах дослідження щодо стійкості та сталості функціонування електронних комунікацій перед кіберзагрозами в умовах побудови «цифрової держави» варто звернути увагу на те, що ЕК є основою ІТС як бізнес-структур, так і державних установ та реєстрів, різного роду центрів обробки даних, інформаційних платформ, а також інформаційних ресурсів. Інакше кажучи, можна констатувати, що ЕК, будучи невід'ємною складовою ІІ та КІІ в цілому, стають уразливими до різного роду та характеру впливів. Стосовно ж фізичного впливу природного та техногенного характеру, то ЕК в умовах створеної мережі ЕК загального користування (завдяки багатооператорському ринку) більш-менш готові до надзвичайних ситуацій. Набагато складнішою є ситуація щодо впливів кібернетичних загроз з огляду на те, що перелік таких загроз є широким і таким, що постійно змінюється та трансформується. Ось чому досить важливим, з урахуванням сучасних викликів, є створення безпечних комунікацій, передусім на рівні кіберзагроз, оскільки питання безперебійності, сталості та стійкості функціонування електронної комунікаційної мережі загального користування, що становлять основу публічних ЕК, є головним завданням постачальників послуг перед користувачами. Так, у ст. 31 «Забезпечення безпеки електронних комунікаційних мереж» Закону України «Про електронні комунікації» від 30 вересня 2020 р. зазначено, що «відповідальність за забезпечення безпеки та сталості електронних комунікаційних мереж загального користування покладається на постачальників мереж та/або послуг електронних комунікацій, крім випадків пошкоджень мереж внаслідок умисних протиправних дій третіх осіб», при цьому «вимоги законодавства щодо безпеки та сталості мереж» повинні визначатися на законодавчому рівні з боку держави, адже лише за умови врахування цих вимог «при розгортанні (створенні) та експлуатації електронних комунікаційних мереж» (Про електронні, 2020) можна досягти відповідного рівня кіберзахисту. Що стосується чинного законодавства, то положеннями Закону України «Про телекомунікації» передбачено «забезпечення сталості телекомунікаційних мереж і управління цими мережами з урахуванням їх технологічних особливостей на основі єдиних норм та правил» (Про телекомунікації, 2004).

Слід зазначити, що завдяки цифровізації та інформатизації всіх сфер суспільства та суспільних відносин «розширюється сукупність суб'єктів, які стають безпосередніми та потенційними об'єктами кіберзагроз як на глобальному, регіональному, національному рівнях, так і на рівні окремих бізнес-структур та інституцій громадянського суспільства, людини і громадянина» (Жиляєв, Семенченко, 2017), де особливого значення набувають ЕК як транспортна складова цифрових потоків у системі сучасних ІІ та КІІ.

Ще одним важливим аспектом використання ЕК є забезпечення населення доступом до електронних адміністративних послуг, перелік яких розширюється. Зазначене повною мірою стосується центрів надання адміністративних послуг, навантаження на які зросло не тільки під впливом карантинних заходів під час проти-

дії пандемії коронавірусу COVID-19, а й через проведення адміністративної реформи, в рамках якої кардинально зменшено кількість районів, у зв'язку із чим втратили статус районні центри багатьох селищ міського типу. Усе це зумовлює зростання навантаження на ЕК через збільшення кількості запитів/звернень від населення на отримання електронних адміністративних послуг та сервісів. Інакше кажучи, навантаження на оброблення, передавання, отримання, зберігання персональних даних громадян та даних баз даних постійно зростає, а разом із цим вони стають усе більш уразливими перед кіберзагрозами. При цьому значний відсоток кіберзагроз генерує кінцеве обладнання (уражене вірусами) громадян, з якого відбувається доступ до ресурсів держави та бізнесу, що також необхідно враховувати.

На сьогодні законодавчо врегульовано та введено в дію такі закони України: «Про захист персональних даних», «Про телекомунікації», «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про адміністративні послуги», «Про реєстр адміністративних послуг», «Порядок ведення Реєстру адміністративних послуг», а також «Концепцію державної політики у сфері цифрової інфраструктури», «Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації», «Стратегію національної безпеки України», «Стратегію Україна 2030Е – Країна з розвинутою цифровою економікою», «Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020)».

Слід зауважити, що «впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту» згідно із Законом України «Про основні засади забезпечення кібербезпеки України» (2017), у рамках якого діє «Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA)» (Про CERT-UA). Крім того, законодавчо визначено перелік «суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки», до якого увійшли «міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом» (Про основні засади, 2017).

Висновки та перспективи подальших досліджень. На підставі результатів дослідження впливу кіберзагроз на функціонування електронних комунікацій (телекомунікацій) в умовах побудови «цифрової держави», слід констатувати, що динаміка розвитку інформаційно-комунікаційних технологій та нового постінформаційного суспільства вимагають від держави та бізнесу перебувати у режимі постійного реагування на нові виклики, які виникають на сучасному етапі розвитку суспільства. Що стосується безпосередньо ЕК, то «для забезпечення можливості оперативно-технічного управління телекомунікаційними мережами загального користування всіх операторів телекомунікацій в умовах надзвичайної ситуації, надзвичайного та воєнного стану» був створений та почав працювати Національний центр оперативно-технічного управління мережами телекомунікацій України (НЦУ) (Про телекомунікації, 2004). При цьому оператори та провайдери електронних комунікацій також взаємодіють з урядовою командою реагування на комп'ютерні надзвичайні події України, НЦУ. Адже ЕК виступає не тільки суб'єктом комунікаційної інфраструктури, а й складовою інформаційно-телекомунікаційних систем та центрів управління ІІ та КІІ у різних сферах економіки. Вважаємо, що велика кількість «суб'єктів, які безпосередньо вживають у межах своєї компетенції заходів щодо забезпечення кібербезпеки» (далі – суб'єкти кібербезпеки), потребує чіткої вертикальної структури (ієрархії) щодо реагування та прийняття рішень під управлінням створеного єдиного національного центру реагування на загрози (ЄНЦРЗ), який би в режимі реального часу тісно взаємодіяв з усіма вказаними вище суб'єктами та виконував функції головного та єдиного центру прийняття рішень щодо реагування на кіберінциденти. Що стосується підпорядкування, то вказаний ЄНЦРЗ доцільно підпорядкувати Раді Національної безпеки і оборони України. Крім того, до оперативного управління та взаємодії мають бути підключені суб'єкти кібербезпеки та оперативного управління в усіх сферах економіки країни.

Але, на наш погляд, головним є навіть не це виходячи з того, що одним із ключових елемен-

тів усіх систем кіберзахисту є людина. Тільки від рівня її професійності та широкого спектру компетентностей (комунікаційної, комп'ютерної, ІТ, цифрової, кібернетичної) залежить високий рівень дієздатності Державного центру кіберзахисту, Урядової команди реагування на комп'ютерні надзвичайні події України, НЦУ, суб'єкти кібербезпеки, а також функціонування центрів надання адміністративних послуг, сайтів органів влади усіх рівнів та компаній тощо. Додатково необхідно наголосити на необхідності підвищення рівня кваліфікації та компетентностей серед населення/громадян. Як зазначають О. Карпенко та Л. Арсенович, при дослідженні питань «державної кіберосвіти та інструментів підвищення рівня цифрової компетентності населення України» «цифрова компетентність населення є основою побудови цифрової економіки та суспільства», а «громадяни України вже перебувають у цифровому світі», тому «лише довгострокова стратегія розвитку кіберосвіти, яка буде зорієнтована на підготовку та спеціалізацію майбутніх поколінь українських користувачів мережевих технологій, дасть змогу забезпечити достатню кількість кваліфікованих кадрів, які професійно володітимуть необхідними цифровими компетенціями (навичками)» (Карпенко, Арсенович, 2020). При цьому така освіта повинна охоплювати всі верстви населення і бути безкоштовною. Так, ці автори запропонували низку заходів, серед яких необхідно звернути увагу на такі, як «забезпечення умов для формування та розвитку державної кіберосвіти населення України на регіональному та місцевому рівнях» з боку місцевої влади та представників бізнесу, «упровадження програм з перекваліфікації (перепідготовки) тимчасово непрацюючих» (Карпенко, Арсенович, 2020) через регіональні відділення центрів зайнятості, а також створення так званих цифрових шкіл вихідного дня, куди б могли приходити цілі родини.

Крім того, було б доцільно використовувати освітній потенціал закладів вищої освіти, де є відповідні напрацювання та вже проводиться навчання за напрямами: інформаційне суспільство, захист інформації, кібербезпека. Вказані навчальні проєкти мають бути обов'язковими в шкільних програмах, щоб підростаюче покоління отримувало базові рівні освіченості та компетентностей, необхідні для якісного входження в кіберпростір. Також варто більш широко залучати до цього різні громадські організації та фонди, які мають відповідну базу та кваліфікацію для підвищення рівня цифрових компетентностей та кіберзахисту.

На державному рівні та рівні ведення бізнесу слід ураховувати, що саме «держава має докласти всіх зусиль, щоб суспільство знало про наявні ризики, а також надавати консультаційну та технологічну підтримку у впровадженні та використанні захищених інформаційно-комунікаційних систем, інфраструктур, платформ тощо» (Україна 2030Е, 2020). Але кіберзахисту вимагають прості громадяни, які використовують ЕК та БКОС для приватно-побутових потреб та розваг. Адже такі комунікації мають масовий характер, зважаючи на широке впровадження проєктів інформатизації «для простої людини». Враховуючи постійні трансформації комунікативних процесів та постійний розвиток техніко-технологічної складової ЕК і відповідне зростання впливу кіберзагроз, питання кіберзахисту ЕК, а отже, питання підвищення рівнів сталості та стійкості вимагає подальших розвідок.

Список використаних джерел

Духовна О. Україна «в цифрі»: напрямки реформування. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ukrayina-v-cifri-napryamki-reformuvannya.html (дата звернення: 07.11.2020).

Жиляєв І., Семенченко А. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. *Стратег. пріоритети.* 2017. № 4 (45). С. 55–63.

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: 07.11.2020).

Карпенко О. В., Арсенович Л. А. Державна кіберосвіта та інструменти підвищення рівня цифрової компетентності населення України. *Вісн. Нац. акад. держ.*

References

Dukhovna, O. Ukraina «v tsyfri»: napriamky reformuvannia (2020). Retrieved from: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ukrayina-v-cifri-napryamki-reformuvannya.html (accesed: 07.11.2020).

Zhyliaiev, I., Semenchenko, A. (2017). Orhanizatsiinopravovi mekhanizmy rozvytku natsionalnoi systemy kiberbezpeky Ukrainy: stan ta perspektyvy [Organizational and legal mechanisms of development of the national cybersecurity system of Ukraine: state and prospects]. *Stratehichni Priorytety.* № 4 (45). P. 55–63 [in Ukrainian].

Zvit pro robotu Natsionalnoi komisii, shcho zdiisniuie rehuliuvannia u sferi zviazku ta informatyzatsii za 2019 rik (2020). Retrieved from: https://nkrzi.gov.ua/index.php?r=site/index&pg=34&id=9088&language=uk (accesed: 07.11.2020).

упр. при Президентові України. Серія «Державне управління». 2020. № 1 (96). С. 95–102.

Нікулеско Д. Торгові марки vs доменні імена: як боротися з кіберсквотингом? URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/torgovi-marki-vs-domenni-imena-yak-borotisya-z-kiberskvotingom.html (дата звернення: 07.11.2020).

Про CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення 10.11.2020).

Про електронні комунікації : Закон України від 30.09.2020 № 934-IX. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68059 (дата звернення: 07.11.2020).

Про затвердження Порядку реєстрації абонентів, які отримують телекомунікаційні послуги без укладення договору в письмовій формі : Рішення НКРЗІ від 28.11.2017 № 607. *Офіц. вісн. України.* 2018. 13 берез. (№ 20). С. 214, 685.

Про захист персональних даних : Закон України. *Голос України.* 2010. 16 верес. (№ 172).

Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відом. Верхов. Ради України.* 2017. № 45. Ст. 403.

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

Про телекомунікації : Закон України від 18.11.2003 № 1280-IV. *Відом. Верхов. Ради України.* 2004. № 12. Ст. 155.

Соснін О. Цифровізація як нова реальність України. URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/ (дата звернення: 07.11.2020).

Україна 2030E – Країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення: 07.11.2020).

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: 07.11.2020).

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

Karpenko, O. V., Arsenovich, L. A. (2020). Derzhavna kiberosvita ta instrumenty pidvyshchenni rivnia tsyfrovoi kompetentnosti naselennia Ukrainy [State cyber education and tools for the ukraine population' digital competence level increasing]. *Bulletin of the NAPA. Series «Public Administration».* Is. 1 (96). P. 95–102 [in Ukrainian].

Nikulesko, D. Torhovi marky vs domenni imena: yak borotysia z kiberskvotynhom? (2020). Retrieved from: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/torgovi-marki-vs-domenni-imena-yak-borotisya-z-kiberskvotingom.html (accesed: 07.11.2020).

Pro CERT-UA. Retrieved from: https://cert.gov.ua/about-us (accesed: 07.11.2020).

Zakon Ukrainy (2020). Pro elektronni komunikatsii : vid 30.09.2020 № 934–IX. Tekst, pidpysanyi Holovoiu Verkhovnoi Rady Ukrainy 13.10.2020. Retrieved from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68059 (accesed: 07.11.2020).

Rishennia NKRZI (2017). Pro zatverdzhennia Poriadku reiestratsii abonentiv, yaki otrymuiut telekomunikatsiini posluhy bez ukladennia dohovoru v pysmovii formi : vid 28.11.2017 № 607. *Ofitsiinyi visnyk Ukrainy.* 2018. 13 march. № 20. P. 214, 685 [in Ukrainian].

Zakon Ukrainy (2010). Pro zakhyst personalnykh danykh : *Holos Ukrainy.* 2010. 16 september № 172 [in Ukrainian].

Zakon Ukrainy (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. *Vidomosti Verkhovnoi Rady Ukraine*. № 45. St. 403 [in Ukrainian].

Rozporiadzhennia Kabinetu Ministriv Ukrainy (2018). Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii vid 17.01.2018 № 67-r. *Uriadovyi kurier.* 2018. 11 may. № 88 [in Ukrainian].

Zakon Ukrainy (2004). Pro telekomunikatsii. *Vidomosti Verkhovnoi Rady Ukrainy.* № 12. St. 155 [in Ukrainian].

Sosnin, O. Tsyfrovizatsiia yak nova realnist Ukrainy (2020). Retrieved from: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny (accesed: 07.11.2020).

Ukraina 2030E – Kraina z rozvynutoiu tsyfrovoiu ekonomikoiu (2020). Retrieved from: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (accesed: 07.11.2020).

Fisun, V. Problemy zakhystu personalnykh danykh: dosvid Ukrainy ta inshykh krain (2020). Retrieved from: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html (accesed: 07.11.2020).

Tsyfrova ekonomika: trendy, ryzyky ta sotsialni determinanty (2020). Kyiv [in Ukrainian].

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. Вплив кіберзагроз на функціонування електронних комунікацій (телекомунікацій) в умовах побудови «цифрової держави». *Вісн. НАДУ. Серія «Державне управління»*. 2020. № 4 (99). С. 84–92.

Стаття надійшла: 25.11.2020

Схвалено до друку: 16.12.2020

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

Citation: Skybun, O. Zh. Vplyv kiberzahroz na funktsionuvannia elektronnykh komunikatsii (telekomunikatsii) v umovakh pobudovy «tsyfrovoi derzhavy» [The influence of cyber threats on the functioning of electronic communications (telecommunications) in conditions of building a «digital state»]. *Bulletin of the NAPA. Series «Public Administration».* Is. 4 (99). P. 84–92 [in Ukrainian].

Article received: 25.11.2020

Accepted: 16.12.2020