DOI https://doi.org/10.30525/978-9934-26-022-3-14

ЗДІЙСНЕННЯ ОПЕРАТИВНО-ТЕХНІЧНОГО УПРАВЛІННЯ ЕЛЕКТРОННИМИ КОМУНІКАЦІЙНИМИ МЕРЕЖАМИ УКРАЇНИ В КОНТЕКСТІ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Скибун О. Ж.

ВСТУП

Стрімкий розвиток науки, техніки та технологій у рамках нового етапу цивілізаційного розвитку суспільства, так званого постіндустріального або інформаційного суспільства формує нові засоби виробництва та виробничі процеси, де інформація отримує статус товару і стратегічного ресурсу, а цифровізація інформації стає важливим фактором домінування сервісної економіки (створення нематеріальних (інформаційних) ресурсів) над виробничою (виробництво матеріальних ресурсів). За таких умов інформаційно-комунікаційні технології, інформатизація та цифровізація починають домінувати над традиційною виробничою сферою. Вказане досить чітко проглядається у контексті подій та заходів у рамках так званих цифрової та четвертої промислової революцій. Додатково до вказаного необхідно зазначити постійно зростаючу роль і вплив на суспільний розвиток такого сучасного явища, як глобалізація, яка завдяки новим технологіям та засобам фізичного переміщення на значні відстані товарів, послуг та людей практично нівелювала такі поняття, як час та відстань. Це призвело до спрощення самих процесів переміщення разом із часом та швидкістю. Так, раніше підготовка та подорож із Європи до Америки займала декілька місяців/тижнів, то тепер це можна здійснити за декілька днів (морем) і декілька годин (літаком). Це створило передумови збільшення рівня мобільності серед людей і разом з цифровізацією бізнесу створило передумови формування нового типу суспільства й економіки, яким не потрібна прив'язка до одного місця (коли бізнес, наукові та виробничі майданчики переміщуються світом у пошуках більш привабливих умов). Це своєю чергою суттєво впливає на взаємини з владою на центральному, регіональному рівнях. Що в кінцевому результаті змінює дискурс комунікацій на рівні людина–суспільство–держава, коли нові цивілізаційні формації та наративи впливають не тільки на оточення людини, а і на неї саму, її світогляд, розуміння дійсності, зовнішній

і внутрішній світи. Вказане відбувається на тлі подальшого збільшення рівня присутності людини у віртуальному (кібернетичному) просторі. Такий тренд споглядається також із боку бізнесу та держави, коли сектори е-бізнесу починають домінувати над реальними (фізичними) секторами економіки. Особливо це стосується сфери надання послуг, а також виконання робіт з інформацією та інформаційними ресурсами. Щодо держави, то основними напрямами є впровадження проєктів інформатизації в рамках е-урядування. Насамперед це стосується надання управлінських послуг в онлайн-режимі. Цьому сприяють розвиток сфери електронних комунікацій: мереж, технологій, обладнання, програмного забезпечення. Так, подальша цифровізація та розвиток сфери електронних комунікацій впливають на інформаційні та комунікативні процеси, коли постійно зростають обсяги та швидкості роботи із цифровими даними (передавання, отримання, оброблення, зберігання, захист тощо). В таких умовах перед державою постають нові виклики, на які необхідно реагувати з позиції навіть не «інформаційного суспільства», а вже «постінформаційного суспільства» або навіть «постекономічного», куди вже крокують передові країни світу, де питанню цифрового розвитку приділяється значна увага та ведеться планомірна робота у зв'язці держава–бізнес. Це пов'язано з тим, що подальший розвиток суспільства тільки прискорюється, а завдяки цифровим технологіям та глобалізації впливає на всі країни світу, тому ті проблеми, які генеруються на рівні високорозвинених країн, дуже швидко хвилями накривають усіх інших, а тому просто «відсидітись» не вдасться нікому, окрім закритих племен Амазонії та Полінезії. Перш за все це стосується кібернетичного сектору, де з'явилися такі нові явища, як: кібернетичні злочини, комп'ютерні віруси, хакери, хакерські атаки не тільки на багатофункціональні кінцеві пристрої окремих громадян, а й на інформаційно-телекомунікаційні системи органів державної влади всіх рівнів, центри обробки даних, системи зв'язку, локальні комп'ютерні мережі і навіть окремі комп'ютери. Разом зі збільшенням рівня цифровізації, комп'ютеризації та інформатизації суспільних відносин та процесів відбувається зростання рівня правочинних дій. А тому слід відзначати, що насамперед уразливою стає вся критична інфраструктура країни (далі – КІІ) разом з окремими об'єктами критичної інфраструктури (далі – ОКІІ), незалежно від форм власності. З огляду на природу загроз можна констатувати, що найбільш уразливою складовою частиною КІІ та ОКІІ є інформаційна інфраструктура (далі – ІІ). Водночас телекомунікації виступають основою інформаційних та комунікативних процесів, базовим елементом інформаційно-телекомунікаційних систем, а також головним елементом цифрових

комунікацій на рівні людина–суспільство–держава. Крім того, телекомунікації є основою для системи державного управління, реагування на надзвичайні ситуації та національної безпеки й оборони. Ось чому стійкість функціонування телекомунікацій в умовах кібернетичних загроз напряму впливає на питання національної безпеки нашої країни.

1. Електронна комунікаційна мережа загального користування та кіберзагрози в рамках «цифрової держави» та «цифрового суспільства»

Натепер відбувається постійне зростання кількості впровадження різних програм та проєктів з інформатизації в рамках «цифрового суспільства» та «цифрової держави». Каталізатором до зростання рівня поширення серед громадян та постійне збільшення залучення широких верств населення до цих програм та проєктів стає розвиток відповідної комунікативної, комунікаційної та інфраструктурної бази для цифрових комунікацій та цифровізації інформаційних (отримання, оброблення, передавання, зберігання та захист інформації) та комунікативних процесів на рівні людина–суспільство–держава. Отже, можна відзначати, що вказане призводить до зростання запиту на електронні комунікаційні послуги високої якості на всій території країни, що досягається надійним та сталим функціонуванням електронної комунікаційної мережі загального користування (далі – ЕКМЗК) в умовах високої стійкості до зовнішніх факторів впливу. До таких нині в основному можна віднести кіберзагрози та надзвичайні ситуації у телекомунікаційних мережах. Така увага до ЕКМЗК викликана тим, що електронні комунікаційні мережі виступають основною транспортною складовою частиною критичної інформаційної інфраструктури (далі – КІІ), а будучи складовим елементом інформаційно-телекомунікаційних систем (далі – ІТС) впливають на стале і безперебійне функціонування системи управління критичною інфраструктурою в усіх сферах життєдіяльності та безпеки країни. Водночас забезпечення безперешкодного доступу всіх верств населення до ЕКМЗК сприяють забезпеченню електронними комунікаційними послугами, доступу до глобальної мережі передачі даних, що дає змогу користуватися послугами на базі електронних комунікацій, отримувати доступ до баз даних, державних сервісів, а також отримувати адміністративні послуги у онлайн-режимі. Наприклад, упродовж «2019 року операторами рухомого (мобільного) зв'язку було значно розширено покриття території України мережами 4G, що дозволило збільшити до 78% частку населення, яке може отримувати послуги мобільного широкосмугового доступу до мережі

Інтернет»[1]. Це ще більше розширює можливості для нових швидкостей та значних обсягів передачі даних за допомогою ЕКМЗК, адже «загальна кількість активних ідентифікаційних телекомунікаційних карток мережі рухомого (мобільного) зв'язку, з яких було здійснено доступ до мережі Інтернет, на кінець 2019 року становила» понад 34 млн од.[2]. Отже, подальший розвиток ЕКМ дає змогу збільшувати свою присутність у віртуальному (кібернетичному) середовищі та отримувати широкий спектр послуг та робіт у різних сферах (економічній, політичній, духовній, гуманітарній), а також у соціальних процесах та комунікаціях. Так, за даними Звіту НКРЗІ за 2019 рік, «широке використання багатофункціональних кінцевих обладнань споживачів, які працюють під управлінням операційних систем (смартфонів, планшетів) та підтримують стандарт LTE» (далі – БКО), сприяє «значному зростанню» кількості «користувачів сучасних електронних сервісів у різних сферах економіки та суспільства»[3]. Тобто це говорить про те, що постійно зростає відсоток використання ЕКМ для передачі даних, а не для голосової телефонії, адже сучасні БКО за своїм функціоналом відійшли дуже далеко від традиційного телефонного апарату, який домінував якихось років п'ятнадцять-двадцять тому. Статистичні дані говорять про те, що «кількість активних ідентифікаційних телекомунікаційних карток мережі рухомого (мобільного) зв'язку» становить 54 млн од., що на третину перевищує кількість усього населення України[4]. Також важлива відмінність сучасного БКО, на яку необхідно звернути увагу, – це високий рівень мобільності й автономності та малі розміри. При цьому спектр завдань, які вирішує сучасне БКО, постійно розширюється та ускладнюється. Так, поєднання людини та машини (в результаті так званих цифрової та четвертої промислової революцій, коли широкого вжитку досягли такі явища, як: штучний інтелект, грід технології, Інтернет речей, smart city, біоінженерія, генетика, нано-технології тощо, відкрило нові горизонти комунікацій як на технічно-технологічному, так і на суспільному рівнях. Сучасний розвиток міжнародних ЕКМ створив світову (глобальну) інформаційну інфраструктуру (далі – ІІ), яка спільно із сучасною транспортною

[1] Звіт про роботу Національної комісії, що здійснює регулювання у сфері зв'язку та інформатизації за 2019 рік. С. 13. URL: https://nkrzi.gov.ua/index.php ?r=site/index&pg=34&id=9088&language=uk (дата звернення: 27.11.2020).

[2] Звіт про роботу Національної комісії, що здійснює регулювання у сфері зв'язку та інформатизації за 2019 рік. С. 19. URL: https://nkrzi.gov.ua/index.php?r=site/ index&pg=34&id=9088&language=uk (дата звернення: 27.11.2020).

[3] Там само. С. 7.

[4] Там само. С. 15, 19.

інфраструктурою (далі – ТІ) формують цифровий порядок денний на глобальному світовому рівні, в якому процеси глобалізації разом із транснаціональними наддержавними структурами починають формувати глобальне громадянське суспільство, глобальну економіку, світовий уряд, загрожуючи тим самим існуванню національних держав, національних економік окремих країн тощо. Тобто ЕКМ поступово перетворилися на інструмент сучасної влади, давши набагато більше можливостей впливу та маніпуляцій як на окрему людину, так і на суспільство загалом, ніж традиційні методи («до цифрові методи») комунікацій. Це можна побачити на рівні сучасних інформаційних політик багатьох країн, які все ширше використовують можливості ЕКМ, інформаційно-комунікаційні технології (далі – ІКТ) та віртуалізацію і глобалізацію суспільства. В таких умовах питання стійкості та сталості функціонування ЕКМ, БКО та ІТС (під впливом зовнішніх чинників, насамперед кібезагроз) впливає на національну безпеку країни загалом, зважаючи на зростання рівня «цифрового суспільства» та «цифрової держави». Поясненням цього є те, що в інформаційному суспільстві інформація отримала ознаки товару та стратегічного ресурсу, а тому захист даних (на рівні держави і бізнесу), а також захист персональних даних (для громадян) стать наріжним каменем сучасної інформаційної державної політики та політики у сфері захисту від кіберзагроз. Щодо обсягів інформації, то, як відзначає С. Левашов, «до 2025 року приблизно 20% усіх даних матимуть критично важливий статус», з яких «близько 10% припаде на сверхкритичну інформацію», оскільки «дані стануть фактором ефективної роботи суспільства і техніки, починаючи від «розумних» медичних інструментів і закінчуючи смарт-гаджетами і безпілотними автомобілями»[5]. Що стосується питань кіберзахисту та кібербезпеки, то вони з часом тільки збільшують свою актуальність в умовах постійного збільшення обсягів інформації, що генерується суспільством, державою та бізнесом. З цього приводу С. Левашов говорить таке: «Сьогодні є істотний розрив між темпами приросту даних і їх захистом», а «у майбутньому цей розрив тільки збільшиться», так, «до 2025 року приблизно 90% усіх даних вимагатимуть певних заходів захисту, проте, за найбільш позитивним прогнозом, лише половина з них буде реально захищена», при цьому «основні витрати, пов'язані зі зберіганням і аналізом великих даних» будуть нести телекомунікаційні компанії,

[5] Левашов С. Будущее Big Data и систем хранения данных. URL: https://www.ramax.ru/press-center/articles/budushchee-big-data-i-sistem-khraneniya-dannykh/ (дата звернення: 05.12.2020).

державні інститути, дослідні центри та виробничі холдинги»[6]. Тобто одним із важливих напрямів із кіберзахисту є створення комплексної системи кіберзахисту із дієвими та ефективними інструментами реагування на кіберподії, а також формування певних заходів для профілактики, адже «зловмисники роблять шкідливе програмне забезпечення з безпрецедентним рівнем складності та впливу», а «зростаюча кількість та різноманітність шкідливих програм підсилюють хаос у ландшафті атак, підриваючи зусилля щодо захисту від загроз», адже «зловмисники та гравці, за якими стоять держави, вже мають необхідні знання й інструменти, щоб зруйнувати критично важливу інфраструктуру і паралізувати життя цілих регіонів»[7]. Тобто можна говорити, що «індустрія» кіберзагроз усе більше отримує ознаки цілеспрямованої спільної дії, які підтримуються урядами певних країн, що несе зростаючу загрозу. Вказане відбувається на фоні збільшення кількості підключень приватного БКО до мережі Інтернет на глобальному рівні, що створює передумови глобальних кіберзагроз, коли національні кордони жодним чином не захищають своїх громадян, адже «шкідливе програмне забезпечення поширювалось трьома способами: приховане завантаження, електронна пошта або через фізичні носії, такі як, наприклад, заражені пристрої пам'яті USB»[8]. Перелік вказаних способів поширення кіберзагроз більшою мірою стосується приватних секторів ІТ-ринку, коли підключення БКО до мережі Інтернет відбувається напряму і здебільшого має символічне програмне забезпечення для захисту від шкідливого програмного продукту. Як відзначається у Річному звіті Cisco з інформаційної безпеки за 2018 рік, «один з найважливіших проривів у ландшафті атак 2017 року полягав у розвитку програм-здирників. Поява мережних програм-здирників усуває потребу в наявності людського елемента під час запуску зловмисних кампаній. Причому здебільшого винагородою є не викуп, а руйнування систем і даних»[9]. Приватний ІТ-сектор досить часто бере програмний продукт шляхом «скачування з Інтернету», тому, «на думку дослідників з компанії Cisco, саморозповсюдне

[6] Левашов С. Будущее Big Data и систем хранения данных. URL: https://www.ramax.ru/press-center/articles/budushchee-big-data-i-sistem-khraneniya-dannykh/ (дата звернення: 05.12.2020).

[7] Cisko 2018. Річний звіт з кібербезпеки. С. 3, 6. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html. (дата звернення: 22.11.2020).

[8] Там само. С. 6.

[9] Cisko 2018. Річний звіт з кібербезпеки. С. 6. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html. (дата звернення: 22.11.2020).

шкідливе програмне забезпечення є не просто актуальною загрозою, але також має потенціал «покласти» Інтернет[10]. Ось чому важливим є своєчасне виявлення кіберзагроз та повідомлення/інформування про них ІТ-спільноту, але при цьому необхідно оперувати достовірними даними, оскільки «в перші години кампанії відчуття необхідності невідкладного реагування з метою оперативної зупинки зловмисників та захисту користувачів може легко призвести до оприлюднення, особливо в соціальних мережах, інформації, яка може вводити її користувачів в оману та не дати їм можливості захистити свої системи»[11]. Тобто неперевірена інформація може створити хаос і паніку, яка тільки сприятиме наслідкам від кіберзагроз. Насамперед це стосується приватного БКО, оскільки державні установи та приватні компанії, які працюють з даними, мають відповідні інструменти для протидії кіберзагрозам. Що стосується ЕКМ, то тут необхідно відзначити, що натепер оператори телекомунікацій усе частіше пропонують споживачам, окрім телекомунікаційних послуг, доступ до контент-послуг, а також самі контент-послуги. Таким чином, оператори телекомунікацій все більше підпадають під вплив кіберзагроз, доставляючи споживачам програмний продукт та контент, будучи його володільцем та несучи відповідальність, оскільки, з одного боку, оператор телекомунікацій виступає як суб'єкт господарювання, який здійснює господарську діяльність з надання телекомунікаційних послуг, а з іншого – як компанія, що надає доступ до контент-послуг, а також самі контент-послуги. Також оператори телекомунікацій на базі власних ЕКМ створюють певні інформаційно-телекомунікаційні системи, потрібні для ведення бізнесу, а тому «відповідальність за забезпечення захисту інформації в системі покладається на власника системи[12]. Крім того, широке впровадження різних проєктів з інформатизації, а також формування послуг із доступу до баз даних вимагає залучення ЕКМ операторів телекомунікацій до інформаційно-телекомунікаційних систем державного рівня (надання адміністративних онлайн-послуг), різноманітних бізнес-проєктів (е-торгівля, е-послуги) та гуманітарні проєкти (телемедицина, е-освіта, е-культура тощо). Вказане вимагає високої якості телекомунікаційних послуг та сталого і стійкого функціонування ЕКМ. Тобто від оператора телекомунікацій вимагається не тільки надання телекомунікаційних послуг, а і забезпечення дієздатності комунікаційної транспортної

[10] Там само. С. 7.
[11] Там само. С. 8.
[12] Про захист інформації в інформаційно-телекомунікаційних системах : Закон України. *Голос України* від 04.08.1994. Ст. 8.

системи на базі ЕКМ у форматі 24/7. Зважаючи на постійно зростаючі обсяги передачі даних з боку суспільства, бізнесу та влади, навантаження на ЕКМ також зростає і тому ІІ та КІІ стають усе більш чутливими до кіберзагроз на ЕКМ. Натепер ЕКМ окремих операторів телекомунікацій формують ЕКМЗК, що накладає на ЕКМ певні протиріччя під час впровадження комплексу заходів із захисту мереж та послуг від кіберзагроз. Так, сучасні інструменти кіберзахисту можуть гарантувати досить високий рівень стійкості та сталості перед кібезагрозами, але це вимагатиме значних матеріально-технічних ресурсів. При цьому потрібно виставляти високі вимоги щодо кіберзахисту до БКО, яке використовується широкими верствами населення. Тобто теоретично можна побудувати таку ЕКМ, яка буде відповідати високим сучасним вимогам щодо стійкості до кіберзагроз, але її вартість буде перевищувати можливості широких верств населення доступу до ЕКМЗК та до загальнодоступних телекомунікаційних послуг, надання яких гарантується державою та встановлюються граничні тарифи для їх надання. Таким чином, може бути створено ситуацію, коли під впливом заходів із кіберзахисту буде здійснювати вплив на свободу слова та плюралізм через блокування певного контенту, який буде визначатись загрозливим. Так, пунктом 4 статті 40 Закону України «Про телекомунікації» відзначається, що «оператори, провайдери телекомунікацій не несуть відповідальності за зміст інформації, що передається їх мережами»[13]. Але при цьому оператори телекомунікацій зобов'язані «вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами»[14], а також «оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами»[15]. При цьому слід відзначити, що не вся інформація, яка циркулює, ЕКМЗК має високий ступінь секретності, а тому і не потребує серйозного захисту щодо її витікання. Водночас оператори телекомунікацій не мають права відслідковувати користувачів стосовно того, який ресурс вони споживають (окрім тих ресурсів, доступ до яких заборонено законодавчо або через суд). Вказаною свободою «серфінгу» у Інтернет-

[13] Про телекомунікації : Закон України. *Відомості Верховної Ради України (ВВР),* 2004, № 12, ст. 40.

[14] Там само, ст. 39.

[15] Там само, ст. 9.

просторі всіх охочих користуються шахраї. Наприклад, «зловмисники, які застосовують технології фішингу та цільового фішингу, постійно вдосконалюють методи соціальної інженерії, що спонукають користувача натиснути на зловмисне посилання або відвідати шахрайські вебсторінки та надати персональні дані чи будь-яку іншу інформацію, яка має велику цінність»[16]. Таким чином, відбувається зараження приватних БКО, які після ураження спонукають подальше поширення кіберзагроз, збільшуючи таким чином навантаження на системи захисту, що функціонують на ІТС, КІІ в усіх сферах суспільства.

2. Національний центр оперативно-технічного управління телекомунікаційними мережами України у системі координат забезпечення кібербезпеки

Питання кібербезпеки та кіберзахисту стають усе більш актуальними та затребуваними на рівні громадян, суспільства, бізнесу та держави, зважаючи на подальші процеси розвитку цифровізації, інформатизації (які відбуваються в рамках «цифрового суспільства» та «цифрової держави»). Довгий час наша країна залишалася на узбіччі масштабних інцидентів, спричинених кіберзлочинами, хоча інтеграція в глобальний інформаційний простір постійно зростала. А тому українське ІТ-середовище виявилося не готовим до стрімких подій, які відбулися в Україні впродовж 2016 та 2017 років, коли, як відзначається фахівцями з кіберзахисту, «нехтування правилами кібербезпеки поставило під загрозу роботу стратегічно важливих об'єктів інфраструктури в Україні»[17]. Саме тоді сталися масовані кібератаки через БКО на ІІ, КІІ та системи управління багатьох державних установ, приватних компаній, а також на приватні БКО, коли «унаслідок 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

[16] Cisko 2018. Річний звіт з кібербезпеки. С. 21. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html. (дата звернення: 22.11.2020).

[17] Новая волна кибератак прокатилась по миру. URL: https://www.dw.com/ru/a-39441129 (дата звернення: 29.11.2020).

з ладу до 10% приватних, урядових і корпоративних комп'ютерів»[18]. З приводу вказаних вище подій 5 липня 2017 Департаментом кіберполіції України було заявлено, що «прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C)», дії якого спричинили до того, що «27.06.2017 о 10 годині 30 хвилин українські державні структури і приватні компанії через вразливості ПЗ «M.E.doc.» (програмне забезпечення для звітності та документообігу) масово потрапили під удар вірусу-шифрувальника (ransomware) Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya)»[19], а саме «протягом вівторка, 27 червня, надійшло понад 200 повідомлень від держустанов, приватних компаній і звичайних громадян про хакерську атаку», коли «масованої атаки, зокрема, зазнали «Укртелеком», «Київ-» і «Дніпроенерго», «Укрзалізниця», аеропорти «Бориспіль» і «Київ», Кабінет Міністрів і МВС України, державний концерн «Антонов», а «Чорнобильська АЕС перейшла через кібератаки на ручний режим радіаційного моніторингу»[20]. У зв'язку з чим «для локалізації масштабної кіберзагрози Національною поліцією України та Службою безпеки України було створено оперативно-технічний штаб, до якого увійшли представники найвідоміших українських та іноземних компаній з кібербезпеки»[21]. Вказані події виявили уразливі сторони у питаннях безпеки, реагування на них та комунікації різних структур, які на державному рівні покликані здійснювати заходи із запобігання та знешкодження кіберзагроз на території України. Так, за інформацією, наданою прес-службою РНБО, «з початку вересня (2020 року) була зафіксована 371 кібератака, яка була віднесена до атак критичного і високого рівня», а загалом «за останні три місяці в Україні було зафіксовано понад 22 мільйони кіберінцидентів», де «за типами кіберінцидентів найбільш поширеними були сканування ресурсів (майже 15,5 млн випадків), bruteforce-атаки (понад 4 млн випадків) і мережеві атаки (майже 1,2 млн випадків)», а «рівень загрози» визначається як «інтегрована оцінка можливостей країни реагувати на

[18] Жиляєв І., Семенченко А. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. Київ. *Стратегічні пріоритети.* № 4 (45), 2017. С. 57.

[19] Прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C). URL: https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/ (дата звернення: 30.11.2020).

[20] Новая волна кибератак прокатилась по миру. URL: https://www.dw.com/ru/a-39441129. (Дата звернення:29.11.2020).

[21] Прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C). URL: https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/ (дата звернення: 30.11.2020).

виклики в кіберпросторі і підтримувати там безпеку»[22]. За даними РНБО, основу кіберінцидентів становили «підрахунок і публікація результатів місцевих виборів; кілька масштабних зливів баз даних зі зламаними акаунтами користувачів (у тому числі українських), виявлена уразливість одного з найбільших виробників мережевого устаткування»[23]. Отже, реагування на кіберінциденти та кіберзагрози вимагає створення ефективної дієздатної системи кіберзахисту на всіх рівнях (національному, регіональному та об'єктовому). Положеннями Закону України «Про основні засади забезпечення кібербезпеки України» визначено перелік «суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки», до якого входять «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»[24]. Вказану тезу ще раз підтримав та озвучив Міністр внутрішніх справ А. Аваков, виступаючи на ZOOM-конференції щодо цифрової трансформації, сказавши таке: «Зважаючи на вимоги сьогодення, підрозділи кібербезпеки мають бути створені у кожному державному органі та установі», бо тільки «потужна система кібербезпеки є надважливою складовою частиною національної безпеки», де «МВС і безпосередньо Департамент кіберполіції Національної поліції є однією з ключових структур цієї системи», а «зважаючи на загрози та визначені пріоритети в їх подоланні, МВС як стейкхолдер кібербезпеки і як супервайзер Національної поліції виступає ініціатором створення на базі Глобального центру взаємодії в кіберпросторі інтеграційного

[22] У РНБО заявили про зростання кіберзагроз. URL: https://ua.korrespondent.net/ukraine/4305521-u-rnbo-zaiavyly-pro-zrostannia-kiberzahroz. (дата звернення: 28.11.2020).

[23] Там само.

[24] Про основні засади забезпечення кібербезпеки України : Закон України. *Відомості Верховної Ради (ВВР)*, 2017, № 45, ст. 5.

майданчика, який би об'єднував усіх ключових гравців кібербезпеки»[25]. Події 2016– 2017 років, пов'язані із потужними кібератаками на ІІ та КІІ, а також на інформаційні ресурси державних установ, бізнес-компаній та великих інфраструктурних компаній стали каталізатором для дій. Так, у рамках формування відповідної державної політики щодо протидії кіберзагрозам було схвалено: Стратегію кібербезпеки України, Доктрину інформаційної безпеки України, Основні засади забезпечення кібербезпеки України, Концепцію створення державної системи захисту критичної інфраструктури, Порядок формування переліку об'єктів критичної інформаційної інфраструктури. Також внесено зміни до деяких законів України, а саме до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» у частині підтвердження відповідності інформаційної системи вимогам із захисту інформації. Крім того, певні положення щодо захисту інформації є у Законі України «Про телекомунікації», а також у Законі України «Про захист персональних даних». Таким чином, можна говорити про сформованість законодавчого поля в частині здійснення заходів із кіберзахисту та захисту інформації.

Натепер питання протидії кіберзагрозам покладені на: Національну поліцію України (департамент кіберполіції), Службу безпеки України (департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, Ситуаційний центр забезпечення кібербезпеки), Адміністрацію Державної служби спеціального зв'язку та захисту інформації (департамент кібербезпеки, департамент захисту інформації), Державну адміністрацію спеціального зв'язку та захисту інформації (Державний центр кіберзахисту, Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA), Національний центр оперативно-технічного управління телекомунікаційними мережами України (далі – НЦУ)). З огляду на зазначене можна виділити сформовані центри, які є нині: Державний центр кіберзахисту, Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA), Ситуаційний центр забезпечення кібербезпеки та кіберполіція. Так, основними завданнями Ситуаційного центру забезпечення кібербезпеки Служби безпеки України є «запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснюються контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством; негласна перевірка

[25] Аваков вважає, що підрозділ кібербезпеки потрібен кожній держустанові. URL: https://www.ukrinform.ua/rubric-society/3106301-avakov-vvazae-so-pidrozdil-kiberbezpeki-potriben-koznij-derzustanovi.html (дата звернення: 25.11.2020).

готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури; забезпечення реагування на кіберінциденти у сфері державної безпеки»[26]. Крім того, в рамках ефективності функціонування Ситуаційного центру забезпечення кібербезпеки для підвищення взаємодії з іншими державними установами, бізнесом та громадянами було «забезпечено з використанням Публічного меморандуму про взаємодію зі Службою безпеки України у сфері відповідального пошуку та розкриття інформації про вразливості інформаційно-телекомунікаційних систем та/або телекомунікаційних мереж реалізацію програми "Bug Bounty" з метою отримання анонімних повідомлень щодо загроз безпечному функціонуванню державних електронних інформаційних ресурсів»[27], а також запропоновано співробітництво в рамках «Публічної угоди про організацію взаємодії з питань обміну інформацією про кібератаки та кіберінциденти з використанням Malware Information Sharing Platform & Threat Sharing "Ukrainian Advantage" між Службою безпеки України та об'єктами критичної інфраструктури, іншими підприємствами, установами, організаціями незалежно від форми власності, а також фізичними особами у питаннях підвищення рівня безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем Користувачів»[28]. У своєму пості у Фейсбуці А. Аваков зазначив такі основні завдання кіберполіції, як: «1. Реалізація державної політики у сфері протидії кіберзлочинності. 2. Протидія кіберзлочинам: у сфері використання платіжних систем: скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток; кеш-трепінг – викрадення готівки з банкомата шляхом встановлення на шатер банкомата спеціальної утримуючої накладки; кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів,

[26] Про Ситуаційний центр забезпечення кібербезпеки Служби безпеки України. URL: https://sbu.gov.ua/ua/pages/330 (дата звернення: 08.12.2020).

[27] Публічний меморандум про взаємодію зі Службою безпеки України у сфері відповідального пошуку та розкриття інформації про вразливості інформаційно-телекомунікаційних систем та/або телекомунікаційних мереж. URL: https://sbu.gov.ua/ua/pages/330. (дата звернення: 22.11.2020).

[28] Публічна Угода про організацію взаємодії з питань обміну інформацією про кібератаки та кіберінциденти з використанням Malware Information Sharing Platform & Threat Sharing "Ukrainian Advantage". URL: https://sbu.gov.ua/ua/pages/330 (дата звернення: 08.12.2020).

що не ініційовані або не підтверджені її держателем; несанкціоноване списанням коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування. У сфері електронної комерції та господарської діяльності: фішинг – виманювання у користувачів Інтернету їхніх логінів та паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування або обміну валюти тощо; онлайн-шахрайство – заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку. У сфері інтелектуальної власності: піратство – незаконне поширення інтелектуальної власності в Інтернеті; кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного TV; у сфері інформаційної безпеки: соціальна інженерія – технологія управління людьми в Інтернет-просторі; мальваре – створення та поширення вірусів і шкідливого програмного забезпечення; протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства; рефайлінг – незаконна підміна телефонного трафіку. 3. Завчасне інформування населення про появу новітніх кіберзлочинів. 4. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини. 5. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів. 6. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності. 7. Участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу»[29]. За інформацією, розміщеною на офіційному вебсайті CERT-UA, до основних завдань віднесено такі: «накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; взаємодія з іноземними та міжнародними організаціями

[29] Пост А. Авакова від 11.10.2015 в Facebook. URL: https://www.facebook.com/arsen.avakov.1/posts/916 452195111554 (дата звернення: 27.11.2020).

з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків; взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам»[30].

Що стосується сфери телекомунікацій, то «для забезпечення можливості оперативно-технічного управління телекомунікаційними мережами загального користування всіх операторів телекомунікацій в умовах надзвичайної ситуації, надзвичайного та воєнного стану» створено «НЦУ»[31]. Серед основних функцій необхідно виділити такі: «здійснює загальний контроль за готовністю та функціонуванням телекомунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану; розробляє моделі можливих надзвичайних ситуацій у телекомунікаційних мережах, а також схеми і механізми розв'язання проблем; взаємодіє з центрами управління мережами, іноземними операторами телекомунікацій, підрозділами оперативно-технічного управління телекомунікаційними мережами спеціальних споживачів, надає їм та отримує від них інформацію про зміну технічного стану трактів, каналів, комутаційних станцій та інших об'єктів управління; організовує оповіщення щодо зміни стану функціонування телекомунікаційних мереж»[32]. Крім того, положеннями «Порядку оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» (затвердженого постановою Кабінету Міністрів України від 29 червня 2004 р. № 812) визначено, що «у разі виникнення надзвичайних ситуацій у телекомунікаційних мережах загальне керівництво системою оперативно-технічного

[30] Про CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення: 05.12.2020).

[31] Про телекомунікації : Закон України. *Відомості Верховної Ради України (ВВР),* 2004, № 12, ст. 29.

[32] Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану : Постанова Кабінету Міністрів України від 29 червня 2004 р. № 812. *Офіційний вісник України* від 16.07.2004 2004 р., № 26, стор. 17, стаття 1696, код акта 29264/2004.

управління телекомунікаційними мережами здійснює постійно діюча галузева комісія з питань техногенно-екологічної безпеки та надзвичайних ситуацій (далі – постійно діюча комісія), яка утворюється і діє як дорадчий орган», а «рішення про переведення системи оперативно-технічного управління телекомунікаційними мережами на надзвичайний режим управління або його припинення після завершення ліквідації наслідків надзвичайної ситуації» приймається «Адміністрацією Держспецзв'язку на основі отриманої від Державної служби з надзвичайних ситуацій інформації та аналізу даних оперативно-інформаційної служби НЦУ про оперативну обстановку у телекомунікаційних мережах, висновку постійно діючої комісії щодо виду, причин, масштабів надзвичайної ситуації у телекомунікаційних мережах, прогнозу її розвитку і наслідків, які впливають на нормальне функціонування мереж», яка «визначає межі зони надзвичайної ситуації у телекомунікаційних мережах»[33]. За такої організації функціонування системи оперативно-технічного управління телекомунікаційними мережами (далі – СОТУ) темпи прийняття рішення, доведення його, а також час формування реакції на надзвичайну ситуацію у телекомунікаційних мережах через кіберінцидент (кіберзагрозу) і здійснення заходів із реагування зовсім не відповідають сучасним реаліям кіберінцидентів, які можуть спричинити надзвичайну ситуацію в телекомунікаційній мережі. А якщо взяти до уваги кібератаки, віднесені до атак критичного і високого рівня, то така організація СОТУ є досить застарілою і тому не зможе інтегруватися у систему кіберзахисту. Це потребує сучасних підходів до формування структури, переліку суб'єктів, їх взаємодії та дієвих інституцій для швидкого реагування із можливістю оперативного управління всіма суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Крім того, необхідно перенести у віртуальний простір функціонування всіх «галузевих комісій з питань техногенно-екологічної безпеки та надзвичайних ситуацій», які приймають рішення у онлайн-режимі про «вид, причини, масштаби надзвичайної ситуації у телекомунікаційних мережах, прогноз її розвитку і наслідків», а також рекомендації щодо заходів з мінімізації збитків, недопущення втрати даних та безперебійності функціонування під час кіберінцидентів та кіберзагроз, які за допомогою сучасних

[33] Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану : Постанова Кабінету Міністрів України від 29 червня 2004 р. N 812. *Офіційний вісник України від* 16.07.2004 2004 р., № 26, стор. 17, стаття 1696, код акта 29264/2004.

механізмів передачі даних передаються як потерпілим від кібератак, так і всім іншим для запобігання та/або мінімізації збитків, недопущення втрати даних та безперебійності функціонування.

Зважаючи на вищевказане, необхідно наголосити на тому, що наявність досить великого переліку організацій, які здійснюють заходи із кіберзахисту, не завжди є синонімом якості, адже питання комунікації та синхронізації дій у реальному часі такого числа організацій не відповідає реаліям сьогодення, коли кіберінцидент може за лічені години паралізувати не тільки ЕКМ, а ІІ та КІІ, спричинивши хаос у системі управління критичною інфраструктурою. Наприклад, як відзначалося вище, «Національною поліцією України та Службою безпеки України було створено оперативно-технічний штаб», який почав реагувати на події (червень 2017 року) постфактум. На ЕКМЗК під час позаштатних ситуацій необхідно збирати постійно діючу комісію. Що стосується НЦУ, то, окрім загальних фраз «щодо взаємодії…», чітко не прописано алгоритм співпраці із Державним центром кіберзахисту, Урядовою командою реагування на комп'ютерні надзвичайні події України (CERT-UA), Ситуаційним центром забезпечення кібербезпеки та кіберполіцією. При цьому відсутні нормативні акти, якими регламентується взаємодія цих усіх структур, які функціонують у системі кіберзахисту, їх сфери діяльності та повноважень під час виявлення та ліквідації різного роду кіберінцидентів та кіберзагроз. У разі повторення повномасштабних кіберінцидентів та кібератак на ІІ, КІІ, БКО оперативно-технічний штаб, розвернутий постфактум, може не допомогти швидко здійснити заходи із кіберзахисту. За таких обставин більш ефективним було б створення на постійній основі одного Національного кризового центру, який би у реальному часі постійно контактував з усіма суб'єктами кіберзахисту. Адже простішими і дешевшими є превентивні заходи, які здійснюються завчасно.

ВИСНОВКИ

Підсумовуючи дослідження питань здійснення оперативно-технічного управління телекомунікаційними мережами України у контексті формування національної системи забезпечення кібербезпеки, необхідно відзначити таке. Натепер електронна комунікаційна мережа виступає основою для поширення цифрової інформації та цифрових інформаційних процесів, формує нові комунікації та комунікативні процеси в усіх сферах суспільства та суспільних відносин. Так, сучасні можливості ЕКМ розширюють спектр послуг на базі телекомунікацій, дають доступ до баз даних, до інформаційних ресурсів державного та приватного рівнів, а також

дають можливості впровадити у системи управління галузями, виробничими сферами та окремими об'єктами інформаційно-аналітичні системи, потужні обчислювальні системи з елементами штучного інтелекту та Інтернету речей.

Так, ЕКМ в епоху інформаційного суспільства і навіть постінформаційного суспільства виступають основою (базисом) для нових комунікацій на рівні людина–суспільство–держава. Без цифровізації, ЕКМ, інформатизації неможливе подальше впровадження результатів цифрової та четвертої революцій. За таких умов питання кіберзахисту стає домінуючим у системі національної безпеки кожної країни загалом, її функціонування та управління. Дослідження системи кіберзахисту нашої країни показало, що на законодавчому рівні питання кіберзахисту врегульовано. Що стосується інституалізації, то в Україні визначено перелік суб'єктів системи кіберзахисту, встановлено перелік ІІ та КІІ. Також розглянуто можливості СОТУ в ЕКМЗК для запобігання кіберінцидентів, захисту від кіберзагроз на ЕКМ для забезпечення їх сталого функціонування в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.

Також було встановлено відсутність дієвого механізму забезпечення захисту від кіберзагроз та надання допомоги населенню у разі настання кіберінциденту високого рівня. Тобто рівень захисту приватного БКО від кіберзагроз залежить від рівня ІТ та кіберкомпетентності його користувача, а беручи до уваги низький загальний рівень цифрових компетентностей, особливо серед населення середнього та старшого віку, це питання є вкрай актуальним. Так, беручи до уваги зростання рівня адміністративних послуг, банківських послуг та комунікацій в онлайн-режимі за допомогою засобів електронних комунікацій, то державі необхідно звернути увагу на приватний сектор, адже проводити масштабні кіберакції можна через соціальні мережі через призване БКО, яке комунікуючи із державними та приватними ІТС, базами даних, виступатиме носієм кіберзагроз. Це треба враховувати, адже кількість БКО тільки зростає.

Що стосується оперативно-технічного управління телекомунікаційними мережами України у контексті формування національної системи забезпечення кібербезпеки, то тут пропонується: переглянути завдання та функції НЦУ; переглянути його роль і місце у СОТУ з огляду на зростання кіберзагроз та широке використання ЕКМ у системі управління критичною інфраструктурою, управлінні державою та національною безпекою; нормативно врегулювати алгоритми взаємодії НЦУ із Державним центром кіберзахисту, Урядовою командою реагування на комп'ютерні надзвичайні події України (CERT-UA), Ситуаційним центром забезпечення кібербезпеки

та кіберполіцією під час виникнення «надзвичайної ситуації» у ЕКМ (виходу з ладу значної частини ресурсів ЕКМ, засобів телекомунікацій (особливо БКО), перевантаження телекомунікаційних мереж (внаслідок кіберциниденту) тощо. Для покращення ефективності функціонування системи кіберзахисту пропонуємо створити на постійній основі Національний кризовий центр, поклавши на нього обов'язки головної інституції у системі кіберзахисту, яка б у реальному часі постійно контактувала та управляла суб'єктами кіберзахисту.

З огляду на те, що подальший розвиток як систем кіберзахисту, так і кіберзлочинів відбуваються постійно, питання оперативно-технічного управління телекомунікаційними мережами України у контексті формування національної системи забезпечення кібербезпеки можна розглядати у контексті подальших розвідок.

АНОТАЦІЯ

У рамках цієї статті проводилось дослідження впливу кіберзагроз на забезпечення оперативно-технічного управління телекомунікаційними мережами України у контексті формування національної системи забезпечення кібербезпеки в умовах подальшої цифровізації, інформатизації та техніко-технологічного розвитку електронних комунікаційних мереж. Було відзначено, що сучасний рівень розвитку електронних комунікацій (постійне збільшення швидкостей та обсягів передачі даних), здешевлення багатофункціонального кінцевого обладнання з операційними системами створили передумови залучення до проєктів «цифрового суспільства» та «цифрової держави» широких верств населення на всій території країни. У зв'язку з цим було відзначено постійне зростання рівня комунікацій у віртуальному (кібернетичному) просторі. Вказане показало зростання ролі електронних комунікаційних мереж у інформаційних системах управління критичною інфраструктурою та у складі інформаційно-телекомунікаційних систем у бізнесі та державі. Це створило передумови збільшення уразливості комунікаційної інфраструктури перед кіберінцидентами та кіберзагрозами як низького, так і високого рівня, коли кіберподії впливають на системи життєдіяльності та управління державою загалом. Дослідження показало досить високий рівень законодавчого врегулювання функціонування системи кіберзахисту та значну кількість суб'єктів кіберзахисту, які перебувають під управлінням державних інституцій. Аналіз функцій та системи оперативно-технічного управління телекомунікаційними мережами показав необхідність реформування діяльності Національного центру оперативно-технічного управління телекомунікаційними мережами України та постійно діючої галузевої

комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій. З урахуванням вищезазначеного було запропоновано практичні напрями для удосконалення оперативно-технічного управління телекомунікаційними мережами України у контексті створення Національного кризового центру, приділення більшої уваги питанням кіберзахисту для приватного багатофункціонального кінцевого обладнання з операційними системами, а також покращення ефективності колективної дії всіх наявних центрів протидії кіберзахисту, що в кінцевому результаті підніме рівень кіберзахисту електронних комунікаційних мереж до рівня, коли вони зможуть ефективно протистояти кіберінцидентам високого рівня.

ЛІТЕРАТУРА

1. Аваков вважає, що підрозділ кібербезпеки потрібен кожній держустанові. URL: https://www.ukrinform.ua/rubric-society/3106301-avakov-vvazae-so-pidrozdil-kiberbezpeki-potriben-koznij-derzustanovi.html (дата звернення: 25.11.2020).
2. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану : Постанова Кабінету Міністрів України від 29 червня 2004 р. № 812. *Офіційний вісник України* від 16.07.2004. 2004 р., № 26, стор. 17, стаття 1696, код акта 29264/2004.
3. Жиляєв І., Семенченко А. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. Київ. *Стратегічні пріоритети*. № 4 (45), 2017. С. 55–63.
4. 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: 27.11.2020).
5. Левашов С. Будущее Big Data и систем хранения данных. URL: https://www.ramax.ru/press-center/articles/budushchee-big-data-i-sistem-khraneniya-dannykh/ (дата звернення: 05.12.2020).
6. Новая волна кибератак прокатилась по миру. URL: https://www.dw.com/ru/a-39441129 (дата звернення: 29.11.2020).
7. Пост А. Авакова від 11.10.2015 в Facebook. URL: https://www.facebook.com/arsen.avakov.1/posts/916 452195111554. (дата звернення :27.11.2020).
8. Прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C). URL: https://cyberpolice.gov.ua/news/ prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/ (дата звернення: 30.11.2020).

9. Про CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення: 05.12.2020).

10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України. *Голос України* від 04.08.1994

11. Про основні засади забезпечення кібербезпеки України : Закон України. *Відомості Верховної Ради (ВВР),* 2017, № 45, ст. 403.

12. Про Ситуаційний центр забезпечення кібербезпеки Служби безпеки України. URL: https://sbu.gov.ua/ua/pages/330 (дата звернення: 08.12.2020).

13. Про телекомунікації : Закон України. *Відомості Верховної Ради України (ВВР)*, 2004, № 12, ст. 155.

14. Публічна Угода про організацію взаємодії з питань обміну інформацією про кібератаки та кіберінциденти з використанням Malware Information Sharing Platform & Threat Sharing "Ukrainian Advantage". URL: https://sbu.gov.ua/ua/pages/330 (дата звернення: 08.12.2020).

15. Публічний меморандум про взаємодію зі Службою безпеки України у сфері відповідального пошуку та розкриття інформації про вразливості інформаційно-телекомунікаційних систем та/або телекомунікаційних мереж. URL: https://sbu.gov.ua/ua/pages/330. (дата звернення: 22.11.2020).

16. У РНБО заявили про зростання кіберзагроз. URL: https://ua.korrespondent.net/ukraine/4305521-u-rnbo-zaiavyly-pro-zrostannia-kiberzahroz (дата звернення: 28.11.2020).

17. Cisko 2018. Річний звіт з кібербезпеки. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html (дата звернення: 22.11.2020).

Information about the author:
Skybun O. Zh.,
Candidate of Science in Public Administration,
Administration of the State Service for Special Communications
and Information Protection
13, Solomianska str., Kyiv, 03110, Ukraine