DOI:**10.33099/2311-7249/2021-42-3-105-110**

УДК 623.486

Сергій Євгенович Гнатюк *(кандидат технічних наук)* [1]
Наталія Дмитрівна Скибун *(кандидат педагогічних наук)* [2]
Євген Олександрович Живило *(кандидат наук з державного управління)* [3]
Сергій Володимирович Волошко *(кандидат технічних наук, с.н.с.)* [3]

1 Адміністрація Державної служби спеціального зв'язку та захисту інформації, Київ, Україна
2 Національний медичний університет ім. О.О. Богомольця, Київ, Україна
3 Національний університет оборони України імені Івана Черняховського, Київ, Україна

ЕЛЕКТРОННІ КОМУНІКАЦІЇ ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ СТАЛОГО ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вивчення ролі електронної мережі Інтернет допускає величезну різноманітність дослідницьких підходів: вона може розглядатися як інформаційна технологія, як психосоціологічний феномен, як спільнота, як фольклор, як універсальна база даних і т.д. З точки зору комунікативних цілей спілкування за допомогою Інтернету має все те різноманіття, яке притаманне іншим різновидам комунікації, - це видно неозброєним оком при першому ж зверненні до змісту електронних повідомлень. В рамках вказаного дослідження було розглянуто електронні комунікації в контексті важливого елементу сталого та безпечного функціонування критичної інфраструктури в Україні. Було відзначено, що електронні комунікації разом із інформаційною інфраструктурою виступають, в сучасних умовах, основою інформаційно-комунікаційних систем управління об'єктів інформаційної критичної та критичної інфраструктур. Рівень впливу електронних комунікацій на стале та безпечне функціонування об'єктів критичної інфраструктури зростає разом із подальшою цифровізацією комунікацій та процесів, запровадження автоматичних та автоматизованих систем управління, використання елементів штучного інтелекту та Інтернету речей.

Ключові слова*: електронні комунікації; інформаційна інфраструктура; інформаційна критична інфраструктуру; критична інфраструктура; оператори телекомунікацій; державно-приватне партнерство; сталість; безпека.*

Вступ

Постановка проблеми. Подальша цифровізація інформації, інформаційних та комунікативних процесів разом із інформатизацією створюють передумови для формування нового цифрового суспільства, цифрової влади та цифрових комунікацій в усіх сферах людського буття (економічна, політична, соціальна та гуманітарна). Так, за домовою інформаційно-комунікаційних технологій, інформаційно-телекомунікаційних систем та глобальної мережі передачі з використанням Інтернету речей, штучного інтелекту відбувається керування багатьма процесами в сферах економіки, надання послуг та управління. Прикладами можуть бути великі інфраструктурні проекти, де на сьогодні керування процесами відбувається на базі величезних автоматизованих систем управління, а саме: проекти smart city, логістика, транспорт, енергетичні мережі тощо. Таким чином інформаційна інфраструктура починає впливати на традиційну критичну інфраструктуру. За таких умов електронні комунікації стають головною транспортною системою на базі якої відбуваються сучасні процеси комунікації, управління та керування. А тому від сталого функціонування електронних комунікацій залежить життєдіяльність не тільки країни в цілому. Отже сталість функціонування критичної інфраструктури починає залежати від сталої роботи інформаційної інфраструктури та електронних комунікацій. Що є досить актуальним в умовах поширення кібернетичних загроз, породжених інформаційним суспільством, коли цифрова революція та четверта промислова революція отримали глобальне поширення та впливу на світову економіку, безпеку та життя людства. В таких умовах критична інфраструктура стала досить вразливою перед сучасними викликами.

Аналіз останніх досліджень і публікацій. На сьогодні питання захисту критичної інфраструктури в умовах кібернетичних загроз, а також сталої роботи комунікаційних мереж є вкрай важливими і тому їм приділяється багато уваги з боку держави, експертів та фахівців, серед яких можна виділити таких: Д. Дубов, Є. Кильчицький, А.Коваленко, Г. Колченко, О. Климчук, О. Резнікова, Н. Слободян, О. Суходоля, Р. Шикас та інші.

Метою статті є обґрунтування продовження заходів щодо забезпечення безпеки та стійкості критичної інфраструктури за умови сталого функціонування інформаційної інфраструктури та комунікаційних мереж.

Виклад основного матеріалу дослідження

Стрімкий розвиток мереж, технологій та обладнання електронних комунікацій стає передумовою подальшого розгортання інформаційно-телекомунікаційних систем, що функціонують як «сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле» [5] для широкого спектру використання в усіх сферах суспільства «інформаційних ресурсів або інформації», де «об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації» [5]. Вказане стає все більш актуальним в рамках збільшення цифровізації інформаційних та комунікативних процесів, широкого впровадження інформатизації, відкритого доступу до баз даних та збільшення ролі інформаційних ресурсів. Так, «інформаційний ресурс» визначається як «систематизована інформація або знання, що мають цінність у певній предметній області і можуть бути використані людиною в своїй діяльності для досягнення певної мети», наприклад під час створення відповідної «інформаційної інфраструктура» [6], яка розглядається як «сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування» [6]. На сьогодні продовжується тенденція постійного збільшення швидкості та обсягів передачі даних, а також обсягів інформації та даних, які зберігаються для подальшої обробки. Сучасною тенденцією є побудова складних систем управління процесами виробництва, управління містом, комунального господарства, енергетичної сфери, банківської системи, надання електронних послуг державними установами з використання ІКТ (наприклад «Держава в смартфоні»), а також розгортання проектів е-демократії, е-парламенту, е-суспільства, е-економіки, е-освіти, е-медицини тощо. Таким чином можна відзначати, що телекомунікаційні мережі виступають важливою «транспортною» основою для розгортання сучасних систем управління об’єктами критичної інфраструктури, де під «критичною інфраструктурою» розглядається система, «що складається з тих об'єктів, послуг та інформаційних систем, які є суттєвими для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, економічного та соціального благополуччя людей, чиї руйнування чи знищення матимуть негативний вплив на національну безпеку, національну економіку, охорону здоров'я, безпеку та ефективне виконання функцій держави» [9]. Важливою особливістю сьогодення є те, що до усіх ризиків, які були в традиційному суспільстві додаються нові, які з’явилися завдяки інформаційному суспільству, глобалізації тощо. І які починають все більше домінувати над усіма іншими, коли «становлення інформаційного суспільства не лише дає змогу будувати більш ефективне та успішне суспільство, але й надає нових імпульсів традиційним загрозам безпеки держави та створює принципово нові складнощі для системи національної безпеки» [8]. Наприклад «через вірус «Petya «А» жертвами хакерської атаки країни-агресора стали Чорнобильська АЕС, аеропорт Харкова, київський метрополітен, українські банки й навіть урядові сайти» [3], а також виникли проблеми у операторів телекомунікацій. Тобто постраждали елементи критичної інфраструктури, через що виникли загрози безпеки життю багатьох людей. Ось чому «активність з боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі все це обумовлює необхідність виробленні рекомендацій щодо коротко- та довгострокових пріоритетів трансформації вітчизняного безпекового сектору з урахуванням вищезазначених трендів» [8]. А тому необхідно відзначити, що «забезпечення інформаційної безпеки у процесі використання інформаційно-комунікаційних технологій є однією з найважливіших умов успішного розвитку інформаційного суспільства» [6]. Враховуючи те, що Україна все більше інтегрується у світову глобальну економіку, глобальні інформаційні системи вона стає більш ураженою від глобальних без пекових загроз. Крім того на сьогодні в країні створюється національний сегмент інформаційної інфраструктури, будуються національні інформаційно-телекомунікаційні системи державного, комерційного та суспільного рівнів, а тому виникає необхідність «забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та органів місцевого самоврядування,

інформаційно-телекомунікаційних систем, які

функціонують в інтересах управління державою, задовольняють потреби оборони та безпеки держави, кредитно-банківських та інших сфер національної економіки, систем управління об'єктами критичної інфраструктури» [6]. Отже для забезпечення високого рівня безпеки необхідно чітко визначати перелік об'єктів, що потребують посиленого захисту. Так, співробітник Центру передового досвіду НАТО з питань енергетичної безпеки Р. Шикас (Литва) наголошує на тому, що «важливість чіткого визначення терміну «критична інфраструктура», який є базовим і від якого залежить організація усього процесу, включаючи питання взаємодії та партнерства» [4], адже в рамках КІ буде визначатися і критична інформаційна інфраструктура (далі – КІІ), а також окремі об'єкти критичної інфраструктури (далі – ОКІ) та об'єкти критичної інформаційної інфраструктури (далі – ОКІІ). На сьогодні в Україні здійснюються заходи для вирішення питань кіберзахисту та кібербезпеки шляхом законодавчого врегулювання широкого спектра питань, які необхідно вирішити для підвищення рівня ефективності захисту та безпеки перш за все на рівні інформаційної інфраструктури (далі – ІІ), адже від стійкості ІІ залежить функціонування критичної інфраструктури (далі – КІ) та безпека країни в цілому. Особливістю сучасного стану речей в Україні є те, що значна кількість ІІ та КІ є приватною і значний відсоток якої знаходиться в управлінні міжнародних транснаціональних компаній. Що стосується телекомунікаційної мережі, то на сьогодні телекомунікаційна мережа загального користування складається із телекомунікаційних мереж приватних операторів телекомунікацій. Тобто виникає ситуація, коли є потреба спільного підходу до питань безпеки ІІ та КІ на загальнодержавному рівні, адже від сталого функціонування об'єктів ІІ та об'єктів КІ залежить життєдіяльність та безпечне існування країни не тільки на національному рівні, а і на глобальному рівні, оскільки до складу КІ входить досить широкий спектр об'єктів промислового, енергетичного, банківського секторів економіки, а також екологічного, водного, природного, що впливають на життя усіх людей.

На сьогодні, в умовах подальшої цифрової революції та діджиталізації усіх процесів та сфер суспільства, до електронних комунікацій як основної транспортної складової починає приділятися все більше уваги через підвищення рівня вимог щодо сталого функціонування самої телекомунікаційної мережі як на фізичному, так і на віртуальному рівнях в умовах подальшого збільшення рівня проникнення елементів цифровізації. Особливо вказане стає чутливим в тих сферах, які формують національну безпеку через сталу роботу та функціонування, в першу чергу, процесів управління в тих сферах, де є в наявності критична інфраструктура, а також в рамках сервісів надання управлінських послуг з боку держави (наприклад «Держава в смартфоні»). Таким чином, можна погодитись із тезою, що сучасний рівень діджиталізації (стан розвитку ІКТ, глобальної мережі передачі даних та інформатизації) створює передумови подальшого збільшення віртуального простору або кібернетичного простору, що «призводить до трансформації державної політики більшості провідних держав в питанні контролю за власним інформаційним (кібер) простором та посиленні яскраво виражених обмежувальних тенденцій» в умовах, коли «кібернетичний простір» «через певну новизну, все ще не повністю нормативно врегульований на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення «акту війни» і можуть бути віднесені до операцій «відмінних від війни» [8]. В таких умовах дійсно виникає потреба у перегляді чинних документів, як регламентують сталість функціонування ІІ, КІІ, КІ на національному рівні. При цьому необхідно враховувати, що в умовах постійного зниження державної частки в структурі ІІ, КІІ та КІ виникає необхідність створення нового рівня державно-приватних партнерських відносин для вирішення проблем сталості та безпеки на рівні національної безпеки. Вказане повним чином стосується операторів електронних комунікацій, комунікаційні мережі яких складають телекомунікаційні мережі загального користування (далі – ТМЗК), адже на сьогодні ринок надання комунікаційних послуг та послуг на базі електронних комунікацій повністю лібералізовано. Так, за інформацією, представленою у Звіті про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації за 2018 рік станом на 01.01.2019 у Реєстрі операторів, провайдерів телекомунікацій зареєстровано понад 6400 операторів та провайдерів телекомунікацій, серед яких – 3600 операторів телекомунікацій [2]. За таких умов багато операторської діяльності гостро постає питання функціонування Ось чому спільне використання ресурсів телекомунікаційних мереж різних операторів (власників) телекомунікацій можливе за умови побудови елементів єдиної системи управління мережами, яка в сучасних умовах може будуватися за централізовано–децентралізованим принципом, де функція управління ресурсами (елементами) телекомунікаційних мереж покладається на операторів (власників) цих мереж, а функція координації спільних дій покладається на відповідний координаційний центр, що повинен забезпечити підготовку оперативних рішень та координацію дій у разі виникнення надзвичайної ситуації, уведення надзвичайного або воєнного стану. Актуальність створення такого координаційного центру збільшується із

зростанням нових елементів ведення «гібридних» бойових дій, кіберінцидентів, терористичних актів в яких віртуальний простір використовується для впливу на фізичний. Адже сучасне комунікаційне обладнання та мережі не можуть функціонувати без програмного забезпечення, а тому разом із проблемами із функціонуванням програмного забезпечення перестають функціонувати і самі комунікаційні мережі, що є складовими інформаційно-комунікаційних систем ІІ, ІКІІ, КІ. На сьогодні в країні створені і функціонують: Національний центр оперативно-технічного управління мережами телекомунікацій України (для забезпечення можливості оперативно-технічного управління телекомунікаційними мережами загального користування всіх операторів телекомунікацій в умовах надзвичайної ситуації, надзвичайного та воєнного стану) (далі – НЦУ) та Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (далі – ДЦКЗ) в рамках якого функціонує Команда реагування на комп'ютерні надзвичайні події України (англ. Computer Emergency Response Team of Ukraine, CERT-UA) для забезпечення кіберзахисту та протидії кіберзагрозам. CERT-UA є акредитованим членом FIRST (англ. Forum for Incident Response and Security Teams, FIRST) та активно взаємодіє з аналогічними командами в усьому світі [7]. Отже на сьогодні в цілому в країні сформовано певні інститути, які повинні виконувати завдання щодо забезпечення сталого та безпечного функціонування ІІ, ІКІІ та КІ. Разом з тим питання сталої та безпечної діяльності операторів та провайдерів телекомунікацій залишається відкритим, оскільки НЦУ функціонує з травня 2019 року. Крім того на сьогодні існує досить складна та тривала з часом процедура реагування на події в частині ТМЗК. Так, «у разі виникнення надзвичайних ситуацій у телекомунікаційних мережах загальне керівництво системою оперативно-технічного 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» [1], а визначення меж «зони надзвичайної ситуації у телекомунікаційних мережах» та прийняття «рішення про переведення системи оперативно-технічного управління телекомунікаційними мережами на надзвичайний режим управління або його припинення після завершення ліквідації наслідків надзвичайної ситуації» на основі отриманої від ДСНС 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» [1]. Такий підхід щодо процедури та механізмів реагування в сучасних умовах є врай неефективним, а тому потребує оптимізації.

Висновки і перспективи подальших досліджень

Підсумовуючи розгляд питань щодо електронних комунікації як важливого елементу сталого функціонування критичної інфраструктури необхідно відзначити таке. Зважаючи на сучасні виклики та загрози, необхідно запроваджувати нові сучасні механізми реагування та прийняття рішень, адже подальший розвиток техніки та технологій тільки збільшує коло механізмів, інструментів та форм впливу на сталість та безпеку електронних комунікацій, які в свою чергу виступають важливим елементом для об’єктів ІІ, ІКІІ, КІ. Виходячи з цього для прискорення процесів від отримання сигнал про подію, вироблення заходів щодо знешкодження та проведення безпосередніх заходів в рамках сталої та безпечної роботи об’єктів ІІ, ІКІ та КІ необхідно переходити від комісій (міжгалузевих, галузевих) із традиційними методами роботи до створення національного координаційного центру з питань сталості та безпеки функціонування об’єктів ІІ, ІКІ та КІ (далі – Координаційний центр з безпеки КІ), який буде: працювати на постійний основі; мати усю повноту влади щодо прийняття рішень, залучення сил, засобів та ресурсів до усунення загрози. До сфери управління якого необхідно залучити в першу чергу підрозділи, що є відповідальними за сталу та безпечну роботу критичної інфраструктури, НЦУ, ДЦКЗ, відповідні підрозділи в ДСНС, Нацполіції, Міноборони тощо. Разом з цим вказаний центр разом із НЦУ та ДЦКЗ повинні оперативно реагувати на звернення приватного сектору (власнику ІІ, ІКІ та КІ), навіть окремих громадян щодо загроз для об’єктів ІІ, ІКІ та КІ, а також надавати всіляку допомогу з питань запобігання загроз для сталої та безпечної роботи.

Крім того, розвиток комунікацій Координаційного центру з безпеки КІ по «горизонталі» із структурними підрозділами ІІ, КІІ, КІ необхідно здійснювати на базі НЦУ та ДЦКЗ в рамках Державно-приватного партнерства в системі забезпечення захисту і стійкості критичної інфраструктури. Для цього необхідно розпочати з: відповідної інформаційної кампанії (ПР-акцій), спрямованої на приватний сектор; з розроблення та затвердження законодавчої бази (основи) для такого партнерства (розпочати із схвалення та впровадження в дію Закону України «Про критичну інфраструктуру» та Концепції державно-приватного партнерства в системі забезпечення захисту і стійкості критичної інфраструктури).

Література

1. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану : постанова Кабінету міністрів України від 29 червня 2004 р. № 12 \ Офіційний вісник України від 16.07.2004 – 2004 р., № 26, стор. 17, стаття 1696, код акту 29264/2004. **2.** Звіт про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації за 2018 рік \ URL: http://www.nerc.gov.ua. **3.** Критична інфраструктура України – під особливою увагою. URL: https://24tv.ua/ru/kritichna_infrastruktura_ukrayini__pid_osoblivoyu_uvagoyu_n1128627. **4.** НІСД провів засідання Міжвідомчої експертної робочої групи на тему «Проблеми розбудови державно-приватного партнерства при захисті критичної інфраструктури». URL: https://niss.gov.ua/en/node/108. **5.** Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 5 липня 1994 року № 80/94-ВР \ Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. **6.** Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження кабінету міністрів України \ Урядовий кур'єр від 13.06.2013 – № 105. **7.** Сайт CERT-UA \ інформація з екрану 13.02.2020. URL: https://cert.gov.ua/. **8.** Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini. **9.** Шикас Рімантас Презентація дослідження та звіту: Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security. URL: https://niss.gov.ua/sites/default/files/2019-04/SikasPresentation.pdf.

ЭЛЕКТРОННЫЕ КОММУНИКАЦИИ КАК ВАЖНЫЙ ЭЛЕМЕНТ УСТОЙЧИВОГО ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

***Сергей Евгеньевич Гнатюк** (кандидат технических наук)* [1]
***Наталия Дмитриевна Скибун** (кандидат педагогических наук)* [2]
***Евгений Александрович Живило** (кандидат наук по государственному управлению)* [3]
***Сергей Владимирович Волошко** (кандидат технических наук, с.н.с.)* [3]

[1] *Администрация Государственной службы специальной связи и защиты информации, Киев, Украина*
[2] *Национальный медицинский университет имени А.А. Богомольца, Киев, Украина*
[3] *Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

Исследование роли электронной сети Интернет допускает большущее обилие исследовательских подходов: оно может рассматриваться как информационная разработка, как психосоциологический парадокс, как общество, как фольклор, как универсальная база данных и т.д. С точки зрения коммуникативных целей общения с помощью Интернета имеет все то многообразие, которое присуще другим разновидностям коммуникации, - это видно невооруженным глазом при первом обращении к содержанию электронных сообщений. В рамках этого исследования были рассмотрены электронные коммуникации в контексте важного элемента устойчивого и безопасного функционирования критической инфраструктуры в Украине. Было отмечено, что электронные коммуникации вместе с информационной инфраструктурой выступают в современных условиях основой информационно-коммуникационных систем управления объектов информационной критической и критической инфраструктур. Уровень влияния электронных коммуникаций на устойчивое и безопасное функционирование объектов критической инфраструктуры растет вместе с последующей цифровизацией коммуникаций и процессов, внедрением автоматических и автоматизированных систем управления, использованием элементов искусственного интеллекта и Интернета вещей.

Ключевые слова. *Электронные коммуникации, информационная инфраструктура, информационная критическая инфраструктура, критическая инфраструктура, операторы телекоммуникаций, государственно-частное партнерство, постоянство, безопасность.*

ELECTRONIC COMMUNICATIONS AS AN IMPORTANT ELEMENT OF SUSTAINABLE FUNCTIONING OF CRITICAL INFRASTRUCTURE

***Sergii Gnatiuk** (Candidate of technical sciences)* [1]
***Natalia Skibun** (Candidate of pedagogical sciences)* [2]
***Yevhen Zhyvylo** (Candidate of Science in Public Administration)* [3]
***Serhii Voloshko** (Candidate of technical sciences, Senior researcher)* [3]

[1] *Department of the State Service for Special Communications and Information Protection, Kyiv, Ukraine*
[2] *Bogomolets national medical university, Kyiv, Ukraine*
[3] *National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*

The study of the role of the electronic network of the Internet allows a huge variety of research approaches: it can be seen as information technology, as a psychosociological phenomenon, as a community, as folklore, as a universal database, etc. From the point of view of communicative purposes, communication via the Internet has all the diversity that is inherent in other types of communication - it is visible to the naked eye when you first turn to the content of electronic messages. In the framework of this study, electronic communications were considered in the context of an important element of sustainable and secure operation of critical infrastructure in Ukraine. It was noted that electronic communications together with the information infrastructure are, in modern conditions, the basis of information and communication systems for the management of information critical and critical infrastructures. The level of impact of electronic communications on the sustainable and safe operation of critical infrastructure is growing with the further digitalization of communications and processes, the introduction of automatic and automated control systems, the use of artificial intelligence and the Internet of Things.

Keywords. *Electronic communications, information infrastructure, critical information infrastructure, critical infrastructure, telecommunications operators, public-private partnership, sustainability, security.*

References

1. Dejaki pytannja operatyvno-tekhnichnogho upravlinnja telekomunikacijnymy merezhamy v umovakh nadzvychajnykh sytuacij, nadzvychajnogho ta vojennogho stanu : postanova Kabinetu ministriv Ukrajiny vid 29 chervnja 2004 r. № 12 \ Oficijnyj visnyk Ukrajiny vid 16.07.2004 – 2004 r., № 26, stor. 17, stattja 1696, kod aktu 29264/2004. **2.** Zvit pro robotu Nacionaljnoji komisiji, shho zdijsnjuje derzhavne reghuljuvannja u sferi zv'jazku ta informatyzaciji za 2018 rik \ URL: http://www.nerc.gov.ua. **3.** Krytychna infrastruktura Ukrajiny – pid osoblyvoju uvaghoju. URL: https://24tv.ua/ru/kritichna_infrastruktura_ukrayini__pid_osoblivoyu_uvagoyu_n1128627. **4.** NISD proviv zasidannja Mizhvidomchoji ekspertnoji robochoji ghrupy na temu «Problemy rozbudovy derzhavno-pryvatnogho partnerstva pry zakhysti krytychnoji infrastruktury». URL: https://niss.gov.ua/en/node/108. **5.** Pro zakhyst informaciji v informacijno-telekomunikacijnykh systemakh. Zakon Ukrajiny vid 5 lypnja 1994 roku № 80/94-VR \ Vidomosti Verkhovnoji Rady Ukrajiny (VVR), 1994, № 31, st.286. **6.** Pro skhvalennja Strateghiji rozvytku informacijnogho suspiljstva v Ukrajini : rozporjadzhennja kabinetu ministriv Ukrajiny \ Urjadovyj kur'jer vid 13.06.2013 – № 105. **7.** Sajt CERT-UA \ informacija z ekranu 13.02.2020. URL: https://cert.gov.ua/. **8.** Suchasni trendy kiberbezpekovoji polityky: vysnovky dlja Ukrajiny. Analitychna zapyska. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini. **9.** Shykas Rimantas Prezentacija doslidzhennja ta zvitu: Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security. URL: https://niss.gov.ua/sites/default/files/2019-04/SikasPresentation.pdf.