

УДК 330.47.65:681

Т. В. Капелюшна,
к. е. н., доцент, доцент кафедри управління інформаційною
та кібернетичною безпекою, Державний університет телекомунікацій
ORCID ID: <https://orcid.org/0000-0001-7490-6751>

DOI: 10.32702/2306-6792.2023.7-8.115

ЗАХИСТ ТА БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ ТА НЕВИЗНАЧЕНОСТІ

Т. Kapeliushna,
PhD in Economics, Associate Professor, Associate Professor of the Department of Information
and Cyber Security Management, State University of Telecommunications

PROTECTION AND SECURITY OF TELECOMMUNICATIONS ENTERPRISES IN THE CONTEXT OF DIGITALIZATION AND UNCERTAINTY

У статті проаналізовано питання захисту та безпеки функціонування підприємств сфери телекомунікацій в умовах цифровізації та невизначеності, яка на сьогодні постала перед Україною. Зауважено, що глобалізація та цифровізація, пандемія, війна посилили важливість розв'язання питань, що стосуються базового соціального забезпечення, котрі визначаються рівнем доступу до інфраструктури (в сфері транспорту, зв'язку, освіти, здоров'я, безпеки).

Відзначено, що телекомунікації забезпечують ефективне управління громадськими і виробничими процесами, розширюють можливості спілкування, навчання та інформованості, дозволяють знижувати витрати виробництва та реалізації продукції, дозволяють ефективно, швидко та більш якісно надавати державні послуги, тим самим підтримуючи інтереси споживачів та господарюючих суб'єктів. Виокремлено інтереси користувачів телекомунікаційних послуг та виділено, що одним із інтересів є питання безпеки.

Виявлено, що у глобальній мережі безпечність даних, конфіденційність інформації, захист персональних даних регламентується Конвенцією 108, статтею 7. Визначено ключові складові (об'єктів і суб'єктів) у формуванні напрямків розвитку телекомунікаційного підприємства в умовах цифровізації та невизначеності; наведено основні послуги для побудови розумних міст, спираючись на дані International Telecommunication Union.

Підкреслено позитивні зрушення для стимулювання роботи у сфері телекомунікацій — пропозицію ДіяCity, за якою надаються переваги компаніям, які реєструються, як резидент та яка слугує стрижнем фінансового захисту та підтримки роботи телекомунікаційних підприємств.

У результаті безпеку підприємств телекомунікаційної сфери визнано, як один із пріоритетних напрямків розвитку країни, оскільки її відносять до критичної інфраструктури та дана сфера є важливою у забезпеченні нормального функціонування та роботи інших підприємств та організацій, економічних суб'єктів у нестійких умовах роботи, крім того телекомунікаційні підприємства слугують підґрунтям для успіху на шляху до цифровізації.

The article pays attention to the protection and security of telecommunication enterprises functioning under the conditions of digitalization and uncertainty that Ukraine faces today. It is noted that globalization and digitalization, pandemic, war have increased the importance of addressing basic social security, which is determined by the level of access to infrastructure (in transport, communications, education, health, security).

It is noted that telecommunications provide effective management of public and production processes, expand the possibilities of communication, education and awareness, allow to reduce the costs of production and sale of products, allow efficient, fast and higher quality public services, thereby supporting the interests of consumers and economic entities. Highlighted the interests of users of telecommunications services and highlighted that one of the interests is the issue of security.

It was revealed that in the global network, data security, confidentiality of information, protection of personal data are regulated by the Convention 108, Article 7. Key components (objects and subjects) in formation of directions of development of telecommunication enterprise in the conditions of digitalization and uncertainty are defined; the basic services for construction of smart cities, based on the data of the International Telecommunication Union, are given.

The positive developments for stimulating work in the telecommunications sector are highlighted — the offer of DiiaCity, under which benefits are given to companies that register as a resident and which serves as a pivot of financial protection and support for the work of telecommunications enterprises.

As a result, the security of telecommunications enterprises is recognized as one of the priorities of the country's development, since it is considered a critical infrastructure and this area is important in ensuring the normal functioning and operation of other enterprises and organizations, economic entities in unstable operating conditions, in addition telecommunications enterprises serve as the basis for success on the road to digitalization.

Ключові слова: безпека телекомунікаційних підприємств, критична інфраструктура, цифровізація, умови невизначеності, безпека та захист підприємств в умовах невизначеності.

Key words: security of telecommunications enterprises, critical infrastructure, digitalization, uncertainty, security and protection of enterprises under uncertainty.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Наразі в сучасних умовах галузь зв'язку відіграє вагому та особливу роль в економічному розвитку країни, формуванні його потенціалу та інформатизації суспільства, формуванні засад сталого розвитку інформаційного суспільства. Суспільство, перебуваючи у інформаційному просторі, маючи вільний доступ до інформаційних джерел, будучи високодіджиталізованим та цифровізованим, має низку переваг у своєму саморозвитку, організації роботи, крім того, має кращі результати при виконанні певних задач або функцій у своїй діяльності.

Глобалізація та цифровізація, пандемія, війна підкреслили важливість питань, що стосуються базового соціального забезпечення, котрі визначаються рівнем доступу до інфраструктури (в сфері транспорту, зв'язку, освіти, здоров'я, безпеки), що є важливим також для господарюючих суб'єктів.

Телекомунікаційна сфера слугує невід'ємним компонентом у діяльності всіх підприємств, крім того, відіграє особливу роль, оскільки забезпечує безперебійне функціонування всіх економічних суб'єктів в нестійких умовах функціонування. Тому захист та безпека діяльності підприємств телекомунікаційної сфери мають розглядатися, як першочергові в умовах цифровізації та невизначеності.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

На сьогодні цифровізація вбачається, як можливість створення додаткових переваг,

вигід у всіх аспектах повсякденного життя та доступ за допомогою інформаційно-комунікаційних технологій до послуг, знань, інформації, даних, а на макрорівні — являється механізмом економічного зростання. Тому низка останніх досліджень науковців була спрямована саме на вплив цифровізації на сучасне існування суспільства, держави та виявленню можливостей та перспектив, які відкриваються за її поширення. Цифровізації присвячені роботи вчених: Вороненко І.В., Каліної І.І., Голобородько А.Ю., Краус Н.М., Краус К.М., Притис В. І., Ганущак Т. В., Макаренко С.М. Питання управління безпекою підприємств висвітлили у своїх працях: Сосновська О.О., Кравчук О.В., Живко З. Б., Черевко О.В., Зачосова Н.В., Живко М. О., Баворовська О.Б., Занора В.О.

Проте, недостатньо дослідженими та опрацьованими залишаються аспекти безпеки функціонування підприємств в умовах цифровізації та невизначеності, які нині склалися та продовжуються ще з часів пандемії, оскільки світ та суспільство, підприємства почали переформатовувати свою роботу у дистанційний формат й активно використовувати інформаційно-комунікаційні технології задля нормального функціонування та можливості продовжувати роботу.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Проаналізувати захист та безпеку функціонування підприємств в умовах цифровізації та невизначеності, що нині сформувався, а також надати рекомендації щодо можливостей посилення безпеки телекомунікаційних підприємств в даних умовах.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Останні кілька років активно обговорювалися ключові питання забезпечення ефективної цифровізації України у середньостроковій перспективі, розроблялися проєкти її поширення на найближчі роки. Причиною активного розгортання питань навколо цифровізації є те, що діджиталізація має сприяти розвитку інформаційного суспільства, засобів масової інформації, "креативного" середовища та "креативного" ринку, використання ІоТ, тощо. Цифровізація України потребує нових форм солідарності, партнерства і співробітництва, регулювання, нових рішень в управлінні безпекою підприємств з урахуванням умов невизначеності.

Цифровізація підприємства, на думку Ганущак Т. В. та Карімова В. Ю., є тим самим рушієм та фактором, що впливає на розвиток економіки [1]. Вороненко І.В. вважає, що в умовах цифровізації економіки підприємства, особливо великі компанії, мають більше уваги приділяти поширенню інформації про свою діяльність, продукцію за допомогою інформаційних ресурсів, а найбільше — соціальних мереж [2]. Розглядаючи парадигми цифрового розвитку в аграрному секторі, Каліна І.І. наголошує на тому, що фактором-стимулятором розвитку є тотальне застосування інформаційних технологій, впровадження яких здійснюється не залежно від наявності потреби та їх доцільності і виокремлює технологічну парадигму розвитку [3]. У роботі Голобородько А.Ю. зазначається, що цифрові трансформації охоплюють різні аспекти і сфери життєдіяльності суспільства — фінансово-економічну, освітню, комунікативну, соціальну, при чому широке використання цифрових продуктів та технологій для задоволення власних потреб сформувало особливості цифрового суспільства [4].

Питанню безпеки в умовах "цифровізації" приділено увагу Кравчук О.В. зокрема, розглянуто виклики цифровізації як проблему безпеки та порушення конфіденційності [5].

Слушно визначено у напрацюваннях Сошовської О.О., що інформаційне забезпечення підприємств зв'язку має на меті задовольнити потреби в інформаційних ресурсах, які являють собою сукупність внутрішніх та зовнішніх інформаційних потоків, необхідних для забезпечення безперервного процесу управління ризиками в системі економічної безпеки підприємств [6].

У праці Чернявського І.Р. та Якименка Ю.М. процес управління інформаційною безпекою

щодо захисту об'єктів інтелектуальної власності розглядається як надійне підґрунтя для забезпечення інноваційного розвитку підприємств малого та середнього бізнесу, наголошено на зростанні важливості, ролі та значущості кібербезпеки для функціонування та розвитку підприємств в умовах нових викликів і загроз [7].

Проблематика безпеки досліджується у роботах Притис В.І., глибинно розглядаються питання безпекоорієнтованого управління підприємствами, а останні напрацювання присвячені проблемі інформаційно-аналітичного забезпечення діяльності підприємства в умовах цифровізації економіки, наголошується на вагомості та ролі інформації в управлінні діяльністю суб'єктом господарювання та загалом її ролі у функціонуванні сучасного підприємства [8].

Краус Н. М., Краус К.М. вбачають, що виробництво і розподіл продукції, робіт/послуг в цифровій економіці — це інформація й способи її передачі, Інтернет-технології, мережеві зв'язки та відповідна інфраструктура, знання, інновації, синергетичні ефекти [9]. Цікавим є результат аналізу Макаренко С.М. щодо технічного обслуговування інфраструктури інформаційно-комунікаційних технологій, підтримки та розвитку програмного забезпечення й забезпечення захисту конфіденційної інформації, що здійснюється лише із залученням фахівців зовнішніх компаній [10]. Однозначно, це засвідчує загрозу порушення конфіденційності, можливості втручання у роботу підприємства, оскільки сторонні особи можуть надавати інформацію зацікавленим сторонам, які являються конкурентами.

Науковці Живко З. Б., Черевко О.В., Зачосова Н.В., Живко М. О., Баворовська О.Б., Занора В.О виділили елементи системи економічної безпеки підприємства такі, як: захист комерційної таємниці та конфіденційності інформації; комп'ютерна безпека; внутрішня безпека; безпека будинків і споруд; фізична безпека; технічна безпека; безпека зв'язку; безпека господарсько-договірної діяльності; безпека перевезень вантажів та осіб; безпека рекламних, культурних, масових заходів, ділових зустрічей та переговорів; протипожежна безпека; екологічна безпека; радіаційно-хімічна безпека; конкурентна розвідка; інформаційно-аналітична робота; експертна перевірка механізму системи забезпечення [11]. Однак, в умовах цифровізації та невизначеності має виокремитися ще кібернетична безпека, оскільки захист інформації (що являє для підприємства цінний

Сприяння інтересам кінцевих користувачів

створення умов для розвитку, доступності і використання електронних комунікаційних мереж високої та надвисокої пропускної здатності, у тому числі мереж фіксованого, мобільного зв'язку та безпроводового доступу, а також електронних комунікаційних послуг	створення умов для отримання максимальної користі під час вибору електронних комунікаційних послуг за ціною і якістю шляхом забезпечення ефективної конкуренції	підтримка безпеки електронних комунікаційних мереж і послуг	забезпечення потреб споживачів в універсальних електронних послугах, у тому числі щодо їх цінової доступності для вразливих соціальних груп споживачів	забезпечення захисту прав та законних інтересів споживачів шляхом нормативно-правового регулювання	забезпечення вибору та рівноцінного доступу до електронних комунікаційних послуг осіб з інвалідністю
--	---	---	--	--	--

Рис. 1. Регулювання питань щодо сприяння інтересам споживачів у сферах електронних телекомунікацій та радіочастотного ресурсу

Джерело: узагальнено та складено за даними [13].

ресурс, який нині формує напрями його роботи та прийняття рішень щодо розвитку та роботи) знаходиться на рівні вищеперелічених елементів безпеки.

Окреслюється питання щодо забезпечення захисту інформації задля безпечного функціонування підприємств в умовах цифровізації, що стрімко шириться під дією нових викликів, які спричинені невизначеністю останніх подій, таких як: пандемія, воєнний стан, геополітичні проблеми.

Основними принципами цифровізації, які сформовано провідними компаніями, є наступні [12]:

— має забезпечувати кожному громадянину рівні можливості доступу до послуг, інформації та знань, що надаються на основі інформаційно-комунікаційних технологій (ІКТ);

— має бути спрямована на створення переваг (вигід) у різноманітних аспектах повсякденного життя;

— є механізмом (платформою) економічного зростання завдяки приросту ефективності, конкурентоздатності, продуктивності від використання цифрових технологій.

Аналізуючи перший принцип, одразу стає зрозумілим, що цифровізаційна розбудова неможлива без інформаційно-комунікаційних

технологій, без доступу до послуг зв'язку, особливо Інтернет. Реалізація вищезгаданого проєкту буде малоімовірною та малоефективною без телекомунікаційної сфери, саме тому розбудова галузі зв'язку є тим підґрунтям, що забезпечить успішність проєкту та сформує цифровий простір із низкою е-послуг та е-сервісів, що надаватимуться на теренах нашої держави.

Телекомунікації забезпечують ефективне управління громадськими і виробничими процесами, розширюють можливості спілкування, навчання та інформованості, дозволяють знижувати витрати виробництва та реалізації продукції, дозволяють ефективно, швидко та якісно надавати державні послуги. Цілком зрозуміло, що під час пандемії, що спричинена COVID активізувалися та інтенсивніше відбувалися процеси цифровізації та цифрової трансформації у всіх сферах.

Телекомунікаційні послуги відіграють неабияку роль у нашому буденному житті: оплата послуг здебільшого здійснюється через мобільні додатки з використанням віртуальних гаманців або платіжних карток; дистанційне навчання та робота (у разі можливості організації її дистанційно) продовжувалися в режимі онлайн за карантину та невизначених умов — через програми для проведення відео конфе-

ренцій: Zoom, Discord, Google Meet, WebEx, Skype, Viber.

Телекомунікаційними послугами користуються у всіх сферах діяльності. Наразі суспільство відчуло їх значущість у своєму житті, крім того, можна стверджувати про зручність та гнучкість організації своєї роботи завдяки перформатуванню стилю свого життя під онлайн режим, оскільки у разі відсутності засобів зв'язку, каналів зв'язку, операторів та провайдерів телекомунікаційних послуг було б складно та довго організовувати свою діяльність в умовах пандемії, в умовах невизначеності, геополітичного напруження, що нині постали перед країнами, а особливо з воєнним станом, введеним в Україні.

Що стосується інституційного забезпечення, ЗУ "Про електронні комунікації" [13] також визначається, яким чином регулюється питання щодо сприяння інтересам кінцевих споживачів телекомунікаційних послуг (рис. 1).

Інтереси користувачів телекомунікаційних послуг регулюються державою та вбачаються у: створенні умов розвитку та доступності використання електронних комунікаційних мереж; конкуренції для можливості обрання електронних комунікаційних послуг за вигідною ціною; наданні універсальних електронних комунікаційних послуг населенню; захисті прав та законних інтересів споживачів послуг; інклюзивному підході у забезпеченні доступу до електронних комунікаційних послуг; безпеці мереж та послуг.

Одним із питань, що стосуються інтересів споживачів телекомунікаційних послуг та регулюються, як ми бачимо є питання безпеки.

В епоху діджиталізації постало питання посилення безпеки та конфіденційності даних, обрання належних заходів безпеки: техніко-технологічного, фізичного, організаційного спрямування. Паралельно цифровізація та доступ до Інтернету, як загальнодоступної послуги, має відповідати наступним принципам: інклюзивність; відсутність дискримінації; та, знову ж таки, безпечність.

Доступ до мережі інтернет має відбуватися безперешкодно, незалежно від того, хто його потребує, де проживає, якої національності, етнічної приналежності, переконань політичних та релігійних, фізіологічних особливостей (інклюзія). Нейтральність вбачається у тому, що користувач сам обирає програмне забезпечення, технології, застосунки, браузер, яким користуватися.

Належна увага має приділятися безпеці, яка забезпечується через захист від несанкціоно-

ваного доступу, протиправного доступу, викривлення даних, їх використання та розповсюдження, що має контролюватися на початковому рівні оператором та контролером. У глобальній мережі безпечність даних, конфіденційність інформації, захист персональних даних регламентується Конвенцією 108, статтею 7 [14].

Дотримання цих принципів є підґрунтям для створення, реалізації та користування перевагами, що надають "цифрові технології".

Отже, телекомунікаційна сфера відіграє особливу роль в розбудові економіки країни, формуванні її економічного потенціалу та інформатизації суспільства. Телекомунікації забезпечують управління громадськими і виробничими процесами, розширюють можливості спілкування, навчання та інформованості, дозволяють суттєво знижувати витрати виробництва та реалізації. Розвиток сфери залежить від розвитку телекомунікаційних підприємств, від того, який їх план розвитку, тому важливо з урахуванням тенденцій розвитку у площині інформатизації, щоб вони рухалися у правильному напрямку, вибудовували ефективну, дієву стратегію свого існування сьогодні та на майбутнє.

Важливо розуміти, що оскільки сфера активно розвивається, необхідно брати до уваги особливості напрямків подальшого розвитку системно: галузь — підприємство — послуга, тобто враховуючи саме трирівневу систему об'єктів життєвого циклу в теорії управління (перший рівень — надорганізаційний (об'єкт дослідження — галузь); другий рівень — організаційний (об'єкт дослідження — організація (підприємство); третій рівень — внутрішньоорганізаційний (об'єкт дослідження — послуга, бренд, знання тощо)).

Слід тримати курс на активну та орієнтовану на довгострокову перспективу стратегію розвитку телекомунікаційного підприємства, яка передбачає високу швидкість реакції на зміни; формування конкурентних переваг; гнучкість; інтенсивність використання факторів виробництва; інноваційність. Враховуючи рівень розвитку об'єктів і суб'єктів ринку телекомунікацій, а також рівень їх впливовості, можемо доцільно виокремити основні із них, які першочергово враховуватимуться при формуванні стратегій або напрямків розвитку телекомунікаційного підприємства (рис. 2).

В умовах воєнного стану в Україні та масованих обстрілів об'єктів критичної інфраструктури відзначається вагомість телекомунікацій та енергетики, чітко окреслюється необхідність

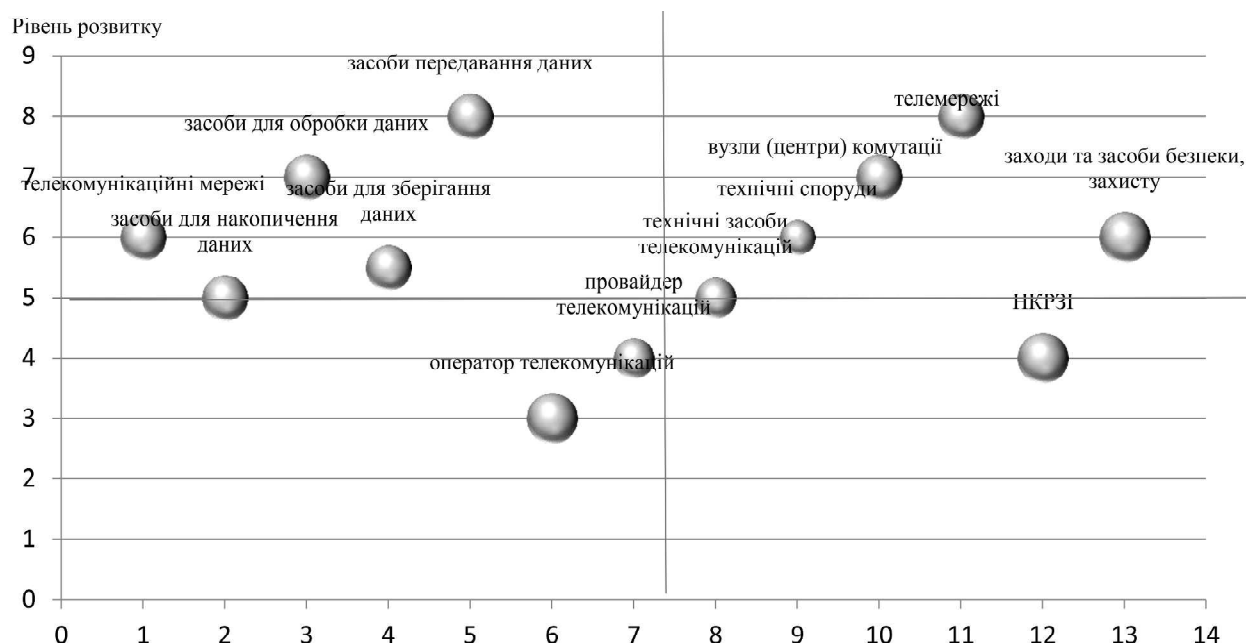


Рис. 2. Визначення ключових складових (об'єктів і суб'єктів) у формуванні напрямків розвитку телекомунікаційного підприємства в умовах цифровізації та невизначеності

Джерело: систематизовано та складено за даними [13; 15].

їх спільної роботи для сталого розвитку. У разі знаходження базових станцій у важкодоступних для подання або відновлення електропостачання районів нині використовуються генератори (як правило дизельні). Актуалізується питання застосування відновлюваної енергетики, гібридних методів для забезпечення безперебійної роботи електростанцій, при чому, окрім стабільного надання телекомунікаційних послуг, усувається втрата доходів, яка могла б виникнути через неможливість надання послуг в тих, чи інших регіонах, які знаходяться без зв'язку. Ще одним позитивним моментом є те, що при використанні відновлюваної енергетики та гібридних методів оператори телекомунікацій знизять витрати за рахунок економії коштів від альтернативних джерел енергії.

За даними International Telecommunication Union основними послугами при побудові розумних міст будуть залишатися наступні [15]:

- енергетичні (живлення від сонячних батарей, автономність від електромережі)
- водопостачання (очищення води)
- складські приміщення та приміщення з охолодженням (зберігання продуктів, напоїв, засобів гігієни, фармацевтична продукція, телекомунікаційне обладнання, прилади)
- роздрібна торгівля (з можливістю прямих продажів)
- доступ до мережі Wi-Fi (різні варіанти підключення до глобальної мережі: 3G, інтернет-провайдера, у разі автономного середови-

ща підключення до Інтернет завдяки ВРТ, супутниковому зв'язку — VSAT, телевізійний ефір),

— цифрові послуги (електронне урядування, дистанційне надання медичних послуг, дистанційна освіта, інтернет-банкінг, інтернет-торгівля, електронна комерція).

— big-data — цифрові та фізичні дані генеруються, зводяться, збираються, зберігаються на єдиній платформі, що є зручно для користувачів та партнерів.

В Україні сильною стороною є динамічний розвиток надання громадянам цифрових послуг через онлайн-сервіс державних послуг "Дія" в будь-який час, незалежно від місцеперебування. Позитивним зрушенням для стимулювання роботи у сфері телекомунікацій є пропозиція ДіяCity, за якою надаються переваги компаніям, підприємствам, які зареєструвавшись, як резидент, матимуть правовий та податковий статус для ведення підприємницької діяльності, побудови відкритого простору функціонування ІТ-компаній, залучення іноземних інвестицій.

Держава всіляко стимулює розвиток ІТ-сфери, іноземним компаніям полегшено процедуру реєстрації як резидента, достатньо зареєструватися відповідно до норм українського законодавства та обрати один із наступних кваліфікованих видів діяльності: розробка та тестування програмного забезпечення (включно з виданням комп'ютерних ігор); видання та роз-

повсюдження програмного забезпечення (SaaS); кіберспорт; навчання комп'ютерній грамотності, програмуванню, тестуванню та технічній підтримці програмного забезпечення; кібербезпека; Research and Development в сфері інформаційних технологій та телекому; Digital-marketing та Ads з використанням програмного забезпечення, що розроблене за участю резидентів; постачання послуг, що пов'язані з обігом віртуальних активів; робототехніка; розробка, запровадження та підтримка рішень міжнародних карткових платіжних систем; виробництво технологічних продуктів для використання оборонній промисловій та побутових сферах; хостинг (хмарні датацентри). Такий підхід щодо спрощення провадження діяльності підприємств сфери ІТ в Україні сприяє кількісному зростанню інноваційних проєктів, пожвавленню інвестиційної привабливості вітчизняних компаній та стартапів; спрощенню умов оподаткування та, відповідно, стимулюванню бізнесу в сфері ІТ; появі альтернативної моделі найму; зростанню питомої ваги високотехнологічної продукції у загальній структурі ВВП.

Слід підкреслити дієвість ДіяCity, станом на лютий 2023 року зареєстровано 485 резидентів, а впродовж повномасштабного вторгнення в Україну агресора, починаючи з 28.02.2022 року зареєстровано 405 компаній, що засвідчує правильність, запропонованих суб'єктам господарювання умов (правових та податкових) для підвищення їх зацікавленості у роботі підприємств сфери [16]. Тобто, запропоновані умови є прийнятними та користуються попитом серед підприємств та організацій, є дієвими та стимулюють до розвитку навіть у надзвичайних умовах, в яких нині перебуває Україна.

Для забезпечення безпечної, безперебійної роботи ІТ сектору наріжним є питання створення гібридних міні-мережевих систем змінного струму, при якій електроенергія передається від джерела енергії безпосередньо в мережу, при одночасній подачі енергії від відновлюваного джерела (попередньо перетворена інверторами) в загальну мережу змінного струму, що дозволить у разі відсутності струму через масовані атаки інфраструктурних об'єктів користуватися енергією із заряджених резервних батарей відновлюваними джерелами. Однозначно, що переформатування станцій у нинішніх невизначених умовах дозволить використовувати накопичену енергію за нормальних умов в пікові години навантаження на мережу. Користь за рахунок гібридних мереж є високою за рахунок енергоефективності та ви-

сокої стійкості, а також можливості керування штучним інтелектом дизель-генератора, що вмикається за потреби через зниження до мінімально допустимого значення напруги акумулятора (зазвичай менше 12%), що й в подальше, мінімізує інвестиційні витрати та оптимізує капітальні та операційні витрати.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних, які формують інформаційну систему загального доступу на сьогодні, в умовах діджиталізації та невизначеності, потребують захисту. Слід звернути увагу на суттєвий вплив операторів і провайдерів телекомунікацій на стан розвитку сфери, адже позитивним вбачається їх збільшення на ринку (нині монополією операторів, низька конкуренція), тобто важливо розвивати конкуренцію. Саме зараз перед Україною відкривається воронка можливостей розширити перелік операторів, які зголосилися б надавати послуги та обладнання для країни, оскільки ситуація щодо електропостачання схвилювала весь світ, що частково намагається зробити країна, запровадивши ДіяCity. Неприпустимо, щоб населення залишалося без зв'язку, більшість інформації отримується саме із глобальної мережі, система оповіщення працює, коли наявний інтернет. Через масовані обстріли, які чиняться з боку країни агресора, відчутними є суттєві порушення у каналах зв'язку, тому безпечність їх роботи є пріоритетною. Тобто, належна увага має приділятися питанням безпеки, що нині забезпечується через розгляд питань, що стосуються інтересів споживачів телекомунікаційних послуг та регулюється національним регулятором у сфері телекомунікацій.

В епоху діджиталізації постало питання посилення безпеки та конфіденційності даних, обрання належних заходів безпеки: техніко-технологічного, фізичного, організаційного спрямування. Цифровізація та доступ до Інтернету, як загальнодоступної послуги, має відповідати наступним принципам: інклюзивність; нейтральність; відсутність дискримінації; безпечність.

Доступ до мережі інтернет має відбуватися безперешкодно, незалежно від того, хто її потребує, де проживає, якої національності, етнічної приналежності, переконань політичних та релігійних та фізіологічних особливостей, що має бути на увазі під інклюзивністю. Нейт-

ральність вбачається у тому, що користувач сам обирає програмне забезпечення, технології, застосунки, браузер, яким користуватися.

Належна увага має приділятися безпеці, яка забезпечується через захист від несанкціонованого доступу, протиправного доступу, викривлення даних, їх використання та розповсюдження, що має контролюватися на початковому рівні оператором та контролером.

Проведене дослідження дозволило визначити безпеку підприємств телекомунікаційної сфери, як один із пріоритетних напрямків розвитку країни, оскільки її відносять до критичної інфраструктури та дана сфера є важливою у забезпеченні нормального функціонування та роботи інших підприємств та організацій, економічних суб'єктів в нестійких умовах роботи, крім того телекомунікаційні підприємства слугують підґрунтям на шляху до цифровізації.

Література:

1. Ганущак Т. В., Карімов В.Ю. Цифровізація на підприємстві як фактор розвитку економіки України. Економіка. Фінанси. Право. 2021. № 4 (2). С. 5—8.

2. Вороненко І. В. Показники функціонування веб-сайтів аграрних компаній як складова цифровізації економіки. Агросвіт. 2019. № 10. С. 53—60.

3. Каліна І. І. Методологічні аспекти дослідження розвитку аграрного сектору в умовах цифровізації. Ефективна економіка. 2020. № 2. URL: http://nbuv.gov.ua/UJRN/efek_2020_2_49. (дата звернення: 10.03.2023).

4. Голобородько А.Ю., Капелюшна Т. В. Формування цифровізації інтегративного розвитку економіки та підприємств, як її елементів. European Journal of Economics and Management. 2022. Volume 8, Issue 6. С. 5—13. URL: https://eujem.cz/wp-content/uploads/2022/eujem_2022_8_6/03.pdf. (дата звернення: 21.01.2023).

5. Кравчук О. В. Державне управління забезпечення державної безпеки в умовах "цифровізації". Теорія та практика державного управління і місцевого самоврядування. 2019. № 1. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2019_1_22. (дата звернення: 17.02.2023).

6. Сосновська О. О. Особливості управління ризиками підприємств сфери зв'язку та інформатизації. Вісник Одеського національного університету. Серія: Економіка. 2019. Т. 24, Вип. 2. С. 64—69.

7. Чернявський І. Р. Якименко Ю. М. Ризикоорієнтований підхід до управління інформаційною безпекою на підприємстві. Сучасний захист інформації. 2022. № 2. С. 38—44.

8. Притис В. І., Кримчак А. А., Гавловська Н. І. Витік інформації як ключова проблема інформаційно-аналітичного забезпечення економічної безпеки підприємства в умовах цифровізації економіки. Бізнес Інформ. 2020. № 10. С. 240—247.

9. Краус К. М., Краус Н. М. Цифровізація в умовах інституційної трансформації економіки: базові складові та інструменти цифрових технологій. Інтелект ХХІ. 2018. № 1. С. 211—214.

10. Макаренко С. М. Особливості інноваційного розвитку промислових підприємств в умовах діджиталізації. Таврійський науковий вісник. Серія: Економіка. 2020. Випуск 3. С. 86—94.

11. Живко З. Б., Черевко О. В., Зачосова Н. В., Живко М. О., Баворовська О. Б., Занора В. О. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник Черкаси: видавець Чабаненко Ю. А., 2019. 120 с.

12. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018—2020 роки та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України; Концепція, План, Заходи від 17.01.2018 № 67 URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>. (дата звернення: 14.02.2023).

13. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 12.03.2023).

14. Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No. 108 allowing the European Communities to accede. URL: <https://www.convention.coe.int/treaty/en/Treaties/Html/108.htm>. (дата звернення: 23.01.2023).

15. International Telecommunication Union https://www.itu.int/dms_pub/itu-d/opb/tnd/D-TND-09-2023-01-PDF-E.pdf (дата звернення: 28.01.2023).

16. Дія.City. Реєстр Дія.City. URL: <https://city.diia.gov.ua/registry/resident>. (дата звернення: 28.02.2023).

References:

1. Hanushchak, T. Karimov, V. (2021), "Digitalization at the enterprise as a factor in the development of the Ukrainian economy", *Ekonomika. Finansy. Pravo*. vol. 4 (2), pp. 5—8.

2. Voronenko, I. (2019), "Indicators of the functioning of agricultural companies' websites as a component of the digitalization of the economy", *Ahrosvit*, vol. 10, pp. 53—60.

3. Kalina, I. (2020), "Methodological aspects of researching the development of the agricultural sector in the context of digitalization", *Efektivna ekonomika*, vol. 2, available at: http://nbuv.gov.ua/UJRN/efek_2020_2_49. (Accessed 10 Mar 2023).

4. Holoborodko, A. and Kapeliushna, T. (2022), "Formation of digitalization of integrative development of the economy and enterprises as its elements", *European Journal of Economics and Management*, vol. 8, Issue 6, available at: https://eujem.cz/wp-content/uploads/2022/eujem_2022_8_6/03.pdf. (Accessed 21 Jan 2023).

5. Kravchuk, O. (2019), "State administration of state security in the context of "digitalization"", *Teoriia ta praktyka derzhavnoho upravlinnia i mistsevoho samovriaduvannia*, vol. 1, available at: http://nbuv.gov.ua/UJRN/Ttpdu_2019_1_22 (Accessed: 17 Feb 2023).

6. Sosnovska, O. (2019), "Peculiarities of risk management in the communications and information sector", *Visnyk Odeskoho natsionalnoho universytetu. Series: Economics*, vol. 24, issue 2, pp. 64—69.

7. Cherniavskiy, I. and Yakymenko, Yu. (2022), "Risk-based approach to information security management at the enterprise", *Suchasnyi zakhyst informatsii*, vol. 2, pp. 38—44.

8. Prytys, V., Krymchak, L. and Havlovska, N. (2020), "Information leakage as a key problem of information and analytical support of economic security of an enterprise in the context of digitalization of the economy", *Biznes Inform*, vol. 10, pp. 240—247.

9. Kraus, K. and Kraus, N. (2018), "Digitalization in the context of institutional transformation of the economy: basic components and tools of digital technologies", *Intelekt XXI.*, vol. 1, pp. 211—214.

10. Makarenko, S. (2020), "Features of innovative development of industrial enterprises in the context of digitalization", *Tavriiskyi naukovyi visnyk*, Series: Economics, vol. 3, pp. 86—94.

11. Zhyvko Z. B. Cherevko, O.V. Zachosova, N.V. Zhyvko, M. O. Bavorovska, O.B. and Zano-ra, V.O. (2019), Organization and management of the enterprise economic security system [Organization and management of the enterprise economic security system], *Vydavets Chabanenko*, Kyiv, Ukraine.

12. The official website of the Verkhovna Rada of Ukraine (2018), "On Approval of the Concept

for the Development of the Digital Economy and Society of Ukraine for 2018-2020 and Approval of the Action Plan for its Implementation. Order of the Cabinet of Ministers of Ukraine; Concept, Plan, Measures", available at: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text> (Accessed: 23 Mar 2023).

13. The official website of the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine" (1981), "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No. 108 allowing the European Communities to accede", available at: <http://ippi.org.ua/vidredaktsiinoi-kolegii-konventsiiya-%E2%84%96-108-radi-%D1%94vropi-%E2%80%99Cpro-zakhyst-osib-u-zv%E2%80%99yazku-z-avtomatizovano> (Accessed: 23 Jan 2023).

14. The official website of International Telecommunication Union (2023), available at: https://www.itu.int/dms_pub/itu-d/opb/tnd/D-TND-09-2023-01-PDF-E.pdf (Accessed: 28 Jan 2023).

15. The official website of Diia.City (2023), "Register Diia.City", available at: <https://city.diia.gov.ua/registry/resident> (Accessed: 28 Feb 2023).

Стаття надійшла до редакції 12.04.2023 р.

www.economy.nayka.com.ua

Електронне фахове видання

**Ефективна
ЕКОНОМІКА**

Виходить 12 разів на рік

Журнал включено до переліку наукових фахових видань України з ЕКОНОМІЧНИХ НАУК (Категорія «Б»)

Спеціальності – 051, 071, 072, 073, 075, 076, 292

e-mail: economy_2008@ukr.net

тел.: (044) 223-26-28

(044) 458-10-73