DOI: 10.46340/eujem.2023.9.1.2

Tetiana Kapeliushna, PhD in Economics
ORCID ID: https://orcid.org/0000-0001-7490-6751
State University of Telecommunications, Kyiv, Ukraine
Alona Goloborodko, PhD in Economics
ORCID ID: https://orcid.org/0000-0001-5416-0526
State University of Telecommunications, Kyiv, Ukraine

CONSIDERATION OF INFORMATION CHALLENGES IN ENTERPRISE SECURITY MANAGEMENT IN TODAY'S UNCERTAIN ENVIRONMENT

Тетяна Капелюшна, к. е. н.
Альона Голобородько, к. е. н.
Державний університет телекомунікацій, Київ, Україна

ВРАХУВАННЯ ІНФОРМАЦІЙНИХ ВИКЛИКІВ ПРИ УПРАВЛІННІ БЕЗПЕКОЮ ПІДПРИЄМСТВ У СЬОГОДЕННИХ НЕВИЗНАЧЕНИХ УМОВАХ

The issues of security and security management of operating enterprises are particularly acute. Challenges such as a pandemic, inflationary processes, political and legislative changes and transformation to the requirements of modernity and digitalization of society, digitalization of the work of all economic entities lead to the need for changes in the approaches to defining security issues and managing the security of enterprises to ensure their normal functioning.

The article notes that enterprises manage to fulfill their functions precisely at the expense of the telecommunications sector, since telecommunications services ensure the functioning of the vast majority of enterprises in the corporate and public sectors. The author emphasizes the importance of server security due to threats to information: violation of its integrity, distortion, which negatively affects the work and performance of enterprises.

The importance of infocommunications and their penetration into all spheres, how telecommunication services improve the quality of life and everyday existence is emphasized.

It is emphasized that information security (as a component of economic security) is currently worthy of attention, so a number of problems and key issues and directions of solution in the formation of security of the information space and the functioning of enterprises are highlighted.

The author establishes the interrelation of current challenges to the safe functioning of enterprises in the digitalized global world and the directions of their solution

The risks (previously identified as likely in the current environment) that are considered to be the most influential are climate change and cyber risks, with energy risks being the fifth most influential due to geopolitical tensions, and the pandemic and its consequences being the fifth most influential. The ranking is carried out, and the three main threats to the safe functioning of enterprises for 2018-2022 are presented.

The author analyzes the share and growth of telecommunications services in exports and imports, emphasizing that exports of telecommunications, computer and information services are growing.

It is emphasized that enterprise security should be achieved through a comprehensive and systematic study of its components, i.e., it should be ensured in general, in all possible directions, taking into account all the challenges and conditions of uncertainty of today.

Keywords: enterprise security, enterprise security management, threats to enterprise functioning, information component, digitalization, uncertainty conditions, threats to enterprise security.

Постановка проблеми. Питання безпеки завжди представляли надвисокий інтерес у держави, домогосподарств, підприємств, оскільки стан її порушення призводить до серйозних наслідків для кожного окремого суб'єкта сектора економіки, що знаходить відображення у порушенні функціонування, дестабілізуючих проявах у вигляді економічних втрат та негативних соціальних явищ.

Впродовж останніх трьох років глобальною проблемою для суспільства була пандемія та інфекційні захворювання, відзначалися негативні наслідки для господарюючих суб'єктів та країн в цілому, оскільки підприємства та організації мали припиняти свою діяльність, переорієнтовувати виробництво, переформовувати свою роботу в режим онлайн, для чого потрібен був час. Реалізувати виконання підприємствами тих чи інших функцій вдалося саме за рахунок телекомунікаційної сфери, через послуги та можливості якої забезпечувалося функціонування переважної більшості підприємств корпоративного та державного сектору.

Дослідження питань безпеки в умовах цифровізації суспільства, нових викликів, які спричинені невизначеністю умов, як пандемії, так і воєнним станом в Україні набувають особливої актуальності та потребують швидкого реагування на загрози, що постають перед функціонуючими підприємствами та виникають на тлі цих подій.

Аналіз основних досліджень і публікацій. Питанням безпеки та упередженню ризиків у функціонуванні підприємств приділили належну увагу у своїх наукових доробках вчені: Чуприн Є.С., Сосновська О.С., Вівчар О.І., Отенко І.П., Гудзь О.Є., Худолій Л М., Гусєва О.Ю., Легомінова С.В., Шкребень Р.П., Кучмєєв О.П., Герасименко О.М., однак, з сьогоденними умовами невизначеності, що чинять руйнівний вплив та дестабілізують функціонування підприємств, питання безпеки підприємств стають наріжними та актуалізуються, потребують врахування нових загроз та небезпек, які виникають під дією вищезгаданої невизначеності.

Мета статті. Дослідити питання управління безпекою підприємств з урахуваннях нових інформаційних викликів, що виникають у сьогоденних невизначених умовах.

Методологія дослідження. Методологічним базисом для дослідження слугували теоретичні положення безпеки функціонування підприємств, нормативно-правові акти, що регулюють захист інформації, наукові роботи вчених, що проводять дослідження у напрямку управління безпекою підприємства. Під час дослідження поставленого питання було використано методи аналізу, синтезу, дедукції, узагальнень та пізнання.

Виклад основного матеріалу. В умовах невизначеності, що складаються останнім часом, підвищується інтерес до посилення безпеки функціонуючих підприємств. Зовнішні втручання, що порушували роботу серверів призвели до того, що більшість інформації зазнала впливу загроз цілісності, підлягала викривленню, що негативно вплинуло на роботу та результати діяльності підприємств. Безпека розглядається в глобальному вимірі, не заточується лише на одному із її елементів, нині передбачається дослідження всіх можливих складових безпеки та їх взаємовпливу. Нові виклики формують нові загрози, тому питання безпечного функціонування підприємств та організацій завжди будуть нагальними та потребуватимуть досліджень, що підтверджується низкою робіт із забезпечення безпеки підприємств. Найчастіше, звісно, у працях науковців уточняються та удосконалюються визначення поняття «безпека підприємства», «економічна безпека підприємства». Так вчений Чуприн Є.С. характеризує економічну безпеку підприємства, як стан підприємства від впливу зовнішніх та внутрішніх дестабілізуючих чинників, що характеризується стабільністю господарської діяльності та дотриманням інтересів підприємства[1]. Вівчар О.І. категоріально визначає економічну безпеку підприємства, як стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування та динамічного науково-технічного і соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам та загрозам[2].

Сосновською О.О. детально розглядаються ризики безпечного функціонування підприємства, зокрема ідентифікуються кадрові загрози зовнішнього і внутрішнього середовища функціонування підприємства, врахування яких, на думку, авторки сприятиме підвищенню адаптивності

[1] Чуприн, Є. (2021). Формування системи забезпечення економічної безпеки підприємств: *автореферат дисертації на здобуття наукового ступеня доктора філософії за спеціальністю 051 «Економіка».* Харків: Харківський національний університет будівництва та архітектури.

[2] Вівчар, О. (2018). Концептуальні засади економічного управління ресурсами на підприємствах: безпекознавчий вимір. *Науковий вісник Ужгородського національного університету,* 51-55.

організаційної структури, покращенню якості управління кадровим потенціалом та створенню унікальної організаційної культури для досягнення безпечного стану кадрової підсистеми й організаційно управлінської стійкості підприємств зв'язку[1].

Детальний огляд інструментів для формування стратегії забезпечення безпеко-орієнтованого розвитку підприємства наведено у роботі Отенко І.П.[2].

На думку Шкребеня Р.П., економічна безпека спрямована на досягнення цілей підприємства, тому це – невід'ємна складова процесу управління розвитком і лише аналіз умов функціонування та можливостей уможливлює відбір та розробку дієвих заходів для безпеки підприємства[3].

У низці робіт прослідковується важливість інституційного забезпечення економічної безпеки для розвитку підприємства, до уваги беруться інтереси екзогенного оточення господарюючого суб'єкта, а саме держави, конкурентів, кредиторів, споживачів, постачальників, інвесторів, партнерів, за їх вподобаннями вибудовується модель поведінки для забезпечення стійкості конкурентної позиції підприємства на ринку. Подібний погляд у Кучеєва О.О., який вважає оточення, як найбільш впливовий елемент у прийнятті рішень для безпечного функціонування підприємства[4].

Вартує уваги праця Герасименко О.М., в якій йдеться про функціонування підприємства в умовах інформаційної економіки, а також концептуально обґрунтовано особливості функціонування системи економічної безпеки підприємства в даних умовах[5]. Належна увага приділена питанням безпеки телекомунікаційних підприємств, зокрема в у роботах Легомінової С.В., Гусєвої О.Ю.[6].

Слід зазначити, що цифровізація та перехід підприємств, організацій у формат онлайн-роботи в умовах, що диктуються невизначеністю, підштовхують на розгляд проблемних питань безпеки інформації, даних, порушення цілісності яких, зростає у діджиталізованому глобальному просторі, а також призводить до деструктивних змін та явищ у роботі підприємства, тим самим порушуючи безпечність його функціонування.

Починаючи із 2019 року, активно провадиться оцифрування послуг, які надаються державою, на порталі «Дія», що розпочав свою роботу у 2020 році як уніфікована платформа доступу бізнесу та громадян до низки державних послуг за єдиними стандартами. Міністерством цифрової трансформації передбачається, що впродовж двох років, до 2024 року, відбудеться оцифрування 100% послуг, які надаються державою. Важливим також є питання підвищення частки ІТ-підприємств у формуванні ВВП держави (на меті досягти 10% галузі ІТ у ВВП країни)[7] й забезпечення транспортної інфраструктури на 95% високошвидкісним та високоякісним інтернетом.

Наразі чітко окреслилось розуміння того, на скільки інфокомунікації проникли у всі сфери, як телекомунікаційні послуги покращують якість життя та повсякденне існування.

Слід зазначити, що Європейським Союзом ще у травні 2019 року започатковано програму «EU4Digital: підтримка цифрової економіки та суспільства у Східному партнерстві»[8], яка розпочата

[1] Сосоновька, О. (2019). Формування системи забезпечення економічної безпеки підприємств: *автореферат дисертації на здобуття наукового ступеня доктора економічних наук.* Київ: Державний університет телекомунікацій.

[2] Отенко, І. Комарков , Д., Шкребень Р. Д. (2018). Стратегічний інструментацій безпеко-орієнтованого розвитку підприємства. *Проблеми економіки*, 235-241.

[3] Шкребень, Р., Харнам, М., Отенко, І. (2020). Формування стратегічного потенціалу безпеко-орієнтованого розвитку підприємства. *Проблеми економіки,* 256-264.

[4] Кучмєєв, О. (2021). Формування економічної безпеки підприємств оптової торгівлі: *автореферат дисертації на здобуття наукового ступеня доктора економічних наук.* Київ: Національний науковий центр «Інститут аграрної економіки».

[5] Герасименко, О. М. (2021). Ризик-орієнтоване управління в системі економічної безпеки підприємства: *автореферат дисертації на здобуття наукового ступеня доктора економічних наук.* Київ: Вищий навчальний заклад «Університет економіки та права «КРОК».

[6] Гусєва, О. Ю., Легомінова, С. В. (2018). Диджиталізація – як інструмент удосконалення бізнес-процесів, їх оптимізація. *Економіка. Менеджмент. Бізнес, 1 (23),* 33-39.

[7] Постанова *Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг 2019* (Кабінет Міністрів України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text> (2022, листопад, 07).

[8] Eufordigital.eu (2020). *EU4Digital: supporting digital economy and society in the Eastern Partnership Cybersecurity guidelines for the Eastern Partner countries* <https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf> (2022, листопад, 11).

з метою: розширення переваг Єдиного цифрового ринку Європейського Союзу для України та інших країн Східного партнерства; економічного росту; створення робочих місць; покращення життя людей та допомоги бізнесу.

Останні події, як спричинені введенням воєнного стану в Україні призвели до адаптації до нових умов невизначеності, пандемія частково загартувала суспільство та пришвидшила цифровізацію суспільства, ніби вимушено, але це дозволило наразі забезпечувати роботу підприємств та організацій, закладів охорони здоров'я та освіти у форматі он-лайн вже з розумінням того, як працювати, які послуги використовувати, які цифрові інструменти та платформи й портали є безпечними та надійними. На сьогодні чітко окреслилося бачення необхідності захисту інформації та безпечної, безперебійної роботи об'єктів критичної інфраструктури, серед яких знаходиться й інформаційно-телекомунікаційних технологій. За Законом України «Про критичну інфраструктуру»[1] серед критично важливих послуг – інформаційні послуги та електронні комунікації. Інформаційний сектор включає інформаційні технології (надання хмарних послуг, забезпечення функціонування систем електронного урядування, забезпечення функціонування систем електронного урядування, розповсюдження ефірного цифрового наземного мовлення з використанням радіочастотного спектра в трьох та більше областях країни), електронні комунікації (забезпечення функціонування точок обміну Інтернет-трафіком, адміністрування адресного простору українського сегмента Інтернету, адміністрування та ведення реєстрів доменних імен верхнього рівня в Інтернеті.

Зростання інформаційних, кібернетичних загроз у цифрову епоху зростає надшвидкими темпами через умови невизначеності (пандемія, геополітичне напруження, воєнний стан), а для бізнесу, функціонуючих підприємств вони несуть невтішні результати. Інформаційна безпека (як складова економічної) наразі є такою, що вартує уваги, так, виокремлюється низка проблем до вирішення, що наведені у табл.1.

Таблиця 1

Виклики та напрями їх усунення у формуванні безпеки інформаційного простору функціонуючого підприємства

Виклики безпеки у інформаційному та кібернетичному просторі	Напрями усунення
Недостатнє фінансування та низька зацікавленість органів влади в аспектах кібербезпеки, Брак кваліфікованих кадрів і ресурсів, а також великі обсяги застарілого обладнання та програмного забезпечення, що становлять високі кіберризики, Уповільнене транскордонне співробітництво Помірне впровадження практик визначених у Директиві ННД, необхідність оновлення стратегії кібербезпеки та пожвавлення розвитку партнерства з технологічними та промисловими партнерами.	• Удосконалення/оновлення Національної стратегії кібербезпеки • Транспозиція Директиви ННД в національні нормативно-правові акти. • Розробка критеріїв для ідентифікації критичної інформаційної інфраструктури • Створення та ведення, оновлення, розширення переліку національних інцидентів, що загрожують безпеці функціонуючих підприємств та організацій • Підвищення стійкості підприємств до інцидентів, • Співробітництво у сфері кібербезпеки • Покращення співпраці між внутрішньодержавними секторами, державним і приватним секторами, а також міжнародного співробітництва. • Національна оцінка кіберризиків з імплементіванням й використанням господарюючими суб'єктами • Прийняття спільної методології та проведення національної оцінки ризиків. • Посилення законодавства у сфері кібербезпеки, гармонізація його з директивами ЄС, створення національних CERT (Computer Emergency Response Team)/ CSIRT та Network and Information Security (NIS)

Складено авторами за результатами досліджень

[1] *Закон України Про критичну інфраструктуру* 2021 (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (2022, листопад, 11).

Проблемні питання формують взаємозв'язок сьогочасних викликів безпечного функціонування підприємств у діджиталізованому глобальному світі з напрямками їх вирішення, що наведено на рис. 1

Рис. 1. Взаємозв'язок сьогочасних викликів безпечного функціонування телекомунікаційних підприємств у діджиталізованому глобальному світі й напрямки їх вирішення

Джерело: складено за результатами досліджень

Комунікаційна та технологічна складова на підприємствах нині є такою, що має убезпечуватися від ризиків та загроз у першу чергу, оскільки кібератака на них призведе до порушення його стабільного функціонування, дестабілізує його розвиток та економічні показники.

Важливість дослідження питань захисту від загроз та ризиків суспільства, держави та підприємств підтверджується низкою експертних оцінювань, серед яких опитування страхових компаній, так у 2020 році у звіті аведено результати ранжування експертами (2600 експертів з 54 країн та приблизно 1000 представників громадськості з 15 різних країн). Серед 25 ризиків, що були попередньо визначені, як вірогідні в сьогоденних умовах й розглядалися, вважаються найбільш впливовими кліматичні зміни та стабільно відзначаються кіберризики, у зв'язку із геополітичною напруженістю виокремлюються енергетичні ризики, пандемія та її наслідки – на п'ятому щаблі.

Ранжування ризиків за вірогідністю їх реалізації за останні 5 років чітко вказує, що в період пандемії гостро стояло питання щодо його вирішення, як на рівні держави, так і господарюючих суб'єктів, оскільки вони мали максимально переформовуватися (по можливості) в онлайн режим функціонування, щоб продовжувати працювати та зменшувати економічні збитки. З урахуванням того, що на зміну однієї невизначеності – пандемії, виникла друга – вторгнення Росії в Україну, в трійці лідерів серед загроз з'являється геополітична, яка на рівні із різким стрімким переходом

Таблиця 2

Ранжування загроз щодо безпечного функціонування підприємств впродовж 2018-2021 рр.

Роки	Зміни клімату	Кібербезпека	Пандемії та інфекційні захворювання	Геополітика
2018	1	2	3	
2019	1	2	3	
2020	2	3	1	
2021	1	2	3	
2022	1	3	5	2

Джерело: складено авторами за [10]

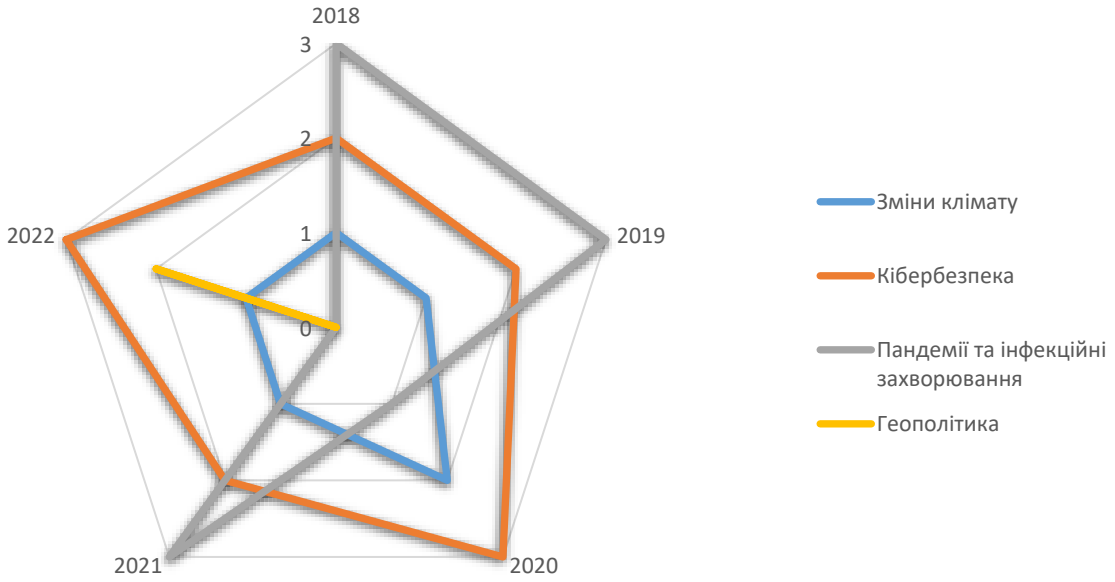

Рис. 2. Трійка основних загроз безпечному функціонуванню підприємств (ранжування за 2018-2022 рр.)

Джерело: візуалізовано авторами за результатами досліджень

у діджиталізований спосіб функціонування привнесла високу ймовірність ризику – кібератак, які націлені на сферу послуг та інфраструктуру. Оскільки умови невизначеності, спонукали підприємства, організації, населення, інституції сприймати кіберризики, як одні із найвагоміших, як ті на, які потрібно звернути чільну увагу й включити в базовий перелік загроз, які потрібно враховувати, щоб забезпечити нормальне функціонування підприємств.

Частина підприємств продовжує працювати у дистанційному форматі, оскільки нині перед країною постали нові виклики, що спричинені вторгненням в на територію України та введенням воєнного стану. Зростають загрози безпеці для підприємств усіх галузей, проводяться кібератаки, які націлені на виведення з робочого режиму критично важливих підприємств та організацій, інфраструктурних об'єктів, платіжних систем. Відбувається посилення дії кіберризиків через геополітичну напруженість та цифровізацію суспільства. Після пандемії загрози безпеці інформації, інформаційного простору виступають на передній план та формують нове сприйняття їх у площині загроз та ризиків безпечного функціонування підприємств. Тому, питання є актуальним, таким, що потребує негайного вирішення.

Також має приділятися належна увага телекомунікаційним підприємствам, оскільки саме ними надаються інфо- та телекомунікаційні послуги. Крім того, аналізуючи питому вагу та приріст телекомунікаційних послуг у експорті та імпорті, можемо зробити висновок, що експорт послуг у сфері телекомунікацій, комп'ютерних та інформаційних послуг зростає (рис. 3).

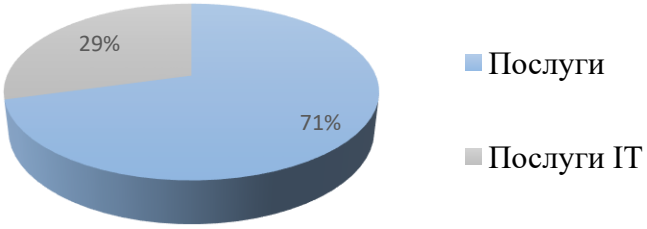

Рис. 3. Питома вага телекомунікаційних, комп'ютерних, інформаційних послуг у загальному обсязі експортованих послуг у 2021 році в Україні

Джерело: складено авторами за джерелом[1]

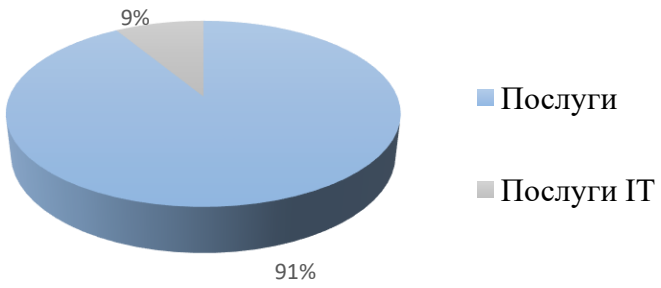

Рис. 4. Питома вага телекомунікаційних, комп'ютерних, інформаційних послуг у загальному обсязі імпортованих послуг у 2021 році в Україні

Джерело: складено авторами за джерелом[2]

Приріст експортованих телекомунікаційних послуг зріс на 26,3 % у 2021 році по відношенню до 2020 року, імпорт теж зріс на 17, 8%. У грошовому виразі обсяг експортованих телекомунікаційних, комп'ютерних, інформаційних послуг резидентами – надавачами країни резидентам за кордон склав 3856, 6 млн. дол. США, а імпорт послуг, наданих резидентам країни нерезидентами-надавачами послуг – 661, 9 млн. дол. США. Питома вага до загального обсягу експортованих послуг сфери IT складає 29, 3% (рис. 3), а імпортованих – 8,7% (рис. 4).

Левова частка, а саме 79% IT послуг, що надавалися за кордон належить комп'ютерним послугам (експортовано на суму 3044,7 млн. долю США)[3].

Варто зауважити, що безпечні умови функціонування телекомунікаціних підприємств дозволяють формувати ефективну протекцію для всіх господарюючих суб'єктів. Але для цього

[1] Міністерство та Комітет цифрової трансформації України (2021). *The Ukrainian IT Sector: An Overview of Publicly Available Data and Gaps in Market Knowledge* <https://drive.google.com/file/d/1hgoJ5n553xJbi6n6X0wwR9sRJWzdMiFU/view> (2022, листопад, 25).
[2] Там само.
[3] Там само.

потрібно розпочинати із захисту функціонування самих інфокумунікаційних підприємств, а саме – з нормативно-правового регулювання безпеки інфокомунікаційного простору.

Законодавчо розгляд та вирішення питання інформаційної, кібербезпеки у всіх секторах економіки розпочалося ще у 2016 році через розроблену Національну Стратегію кібербезпеки. За останні роки прийнято низку національних нормативно-правових актів, пов'язаних з безпекою функціонування підприємств, організацій, інституцій в інформаційному та телекомунікаційному просторі: затвердження «Положення про захист інформації та кіберзахист учасниками платіжного ринку»[1] , «Про основні засади забезпечення кібербезпеки України»[2], «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації»[3], «Про реалізацію експериментального проекту із створення, впровадження та забезпечення функціонування Єдиної цифрової інтегрованої інформаційно-аналітичної системи управління процесом відбудови інфраструктури»[4], «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України»[5], «Про затвердження Порядку використання коштів з рахунка Міністерства цифрової трансформації для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави»[6], «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів»[7], «Про хмарні послуги»[8], Деякі питання функціонування Національної телекомунікаційної мережі[9]. Також передбачається здійснювати захист даних (зокрема персональних) Порталу Дія від несанкціонованого доступу, знищення, модифікації.

Беззаперечно, безпечне функціонування підприємства формує його імідж, впливає на конкурентоспроможність, дозволяє отримувати заплановані результати діяльності, розвиватися та посилювати свої позиції на ринку.

---

[1] *Постанова Положення про захист інформації та кіберзахист учасниками платіжного ринку, 2021* (Національний Банк України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/v0043500-21#Text> (2022, листопад, 25).

[2] *Закон України Про основні засади забезпечення кібербезпеки України, 2017* (Верховна Рада України). *Офіційний -сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (2022, листопад, 21).

[3] *Закон України Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації, 2022* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/2801-20#Text> (2022, листопад, 24).

[4] Постанова Кабінету Міністрів України *2022 Про реалізацію експериментального проекту із створення, впровадження та забезпечення функціонування Єдиної цифрової інтегрованої інформаційно-аналітичної системи управління процесом відбудови інфраструктури* (Верховна Рада України). Офіційний веб-сайт Верховної Ради України. <https://zakon.rada.gov.ua/laws/show/1286-2022-%D0%BF#Text> (2022, листопад, 18).

[5] *Постанова Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України, 2022* (Національний банк України). *Офіційний сайт Національного банку України* <https://bank.gov.ua/ua/legislation/Resolution_12082022_178> (2022, листопад, 19).

[6] Постанова *Про затвердження Порядку використання коштів з рахунка Міністерства цифрової трансформації для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави, 2022* (Кабінет Міністрів України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/751-2022-%D0%BF#Text> (2022, листопад, 27).

[7] *Закон України Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів, 2022* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/2130-20#Text> (2022, листопад, 29).

[8] *Закон України Про хмарні послуги, 2022* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text> (2022, листопад, 18).

Прослідковується, що безпека підприємства досягається шляхом комплексного та системного вивчення її складових, тобто має забезпечуватися в цілому, за всіма можливими напрямками, якщо узагальнити: економічної безпеки, матеріальної (фізичної) безпеки, інформаційної безпеки. З інформатизацією та цифровізацією суспільства все більшу роль відіграє у безпеці функціонуючих підприємств та організацій захист інформації та даних. Саме тому подальші дослідження будуть націлені на комплексне вивчення складових безпеки в умовах діджиталізованого та глобалізованого функціонування підприємств з практичним застосуванням результатів досліджень на функціонуючих підприємствах для безпечного їх існування та розвитку, з урахуванням інформаційних ризиків, особливо у сфері телекомунікацій.

References:

1. Chuprin, E. (2021). Formuvannya systemy zabezpechennya ekonomichnoyi bezpeky pidpryyemstv [Formation of the system of ensuring the economic security of enterprises]: *avtoreferat dysertatsiyi na zdobuttya naukovoho stupenya doktora filosofiyi za spetsialnistyu 051 «Ekonomika»* [the dissertation author's abstract for obtaining the scientific degree of Doctor of Philosophy in the specialty 051 "Economics"]. Kharkiv: Kharkiv National University of Construction and Architecture. [in Ukrainian].
2. Vivchar, O. (2018). Kontseptualni zasady ekonomichnoho upravlinnia resursamy na pidpryiemstvakh: bezpekoznavchyi vymir [Conceptual Bases of Economic Management of Resources at Enterprises: Security Studies Dimension]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu* [Scientific Bulletin of Uzhhorod National University], 51-55 [in Ukrainian].
3. Sosonovka, O. (2019). Formuvannya systemy zabezpechennya ekonomichnoyi bezpeky pidpryyemstv [Formation of the system for ensuring the economic security of enterprises]: *avtoreferat dysertatsiyi na zdobuttya naukovoho stupenya doktora ekonomichnykh nauk* [the dissertation author's abstract for obtaining the scientific degree of Doctor of Economic Sciences]. Kyiv: State University of Telecommunications. [in Ukrainian].
4. Otenko, I. Komarkov , D., Shkreben R.. (2018). *Stratehichnyi instrumentatsii bezpeko-oriientovanoho rozvytku pidpryiemstva* [Strategic tools for security-oriented development of the enterprise]. *Problemy ekonomiky* [Problems of Economics], 235-241. [in Ukrainian].
5. Shkreben, R., Kharnam, M., Otenko, I. (2020). *Foruvannia stratehichnoho potentsialu bezpeko-oriientovanoho rozvytku pidpryiemstva* [Formation of the strategic potential of security-oriented development of the enterprise]. *Problemy ekonomiky* [Problems of economy], 256-264 [in Ukrainian].
6. Kuchmeev, O. (2021). Formuvannya ekonomichnoyi bezpeky pidpryyemstv optovoyi torhivli [Formation of economic security of wholesale trade enterprises]: *avtoreferat dysertatsiyi na zdobuttya naukovoho stupenya doktora ekonomichnykh nauk* [the dissertation author's abstract for obtaining the scientific degree of Doctor of Economic Sciences. Kyiv: National Scientific Center "Institute of Agrarian Economy". [in Ukrainian].
7. Herasimenko, O. M. (2021). Ryzyk-oriyentovane upravlinnya v systemi ekonomichnoyi bezpeky pidpryyemstva [Risk-oriented management in the system of economic security of the enterprise]: *avtoreferat dysertatsiyi na zdobuttya naukovoho stupenya doktora ekonomichnykh nauk* [the dissertation author's abstract for obtaining the scientific degree of Doctor of Economic Sciences]. Kyiv: University of Economics and Law "KROK" Higher Educational Institution. [in Ukrainian].
8. Husieva, O. Iu., Lehominova, S. V. (2018). *Didzhytalizatsiia – yak instrument udoskonalennia biznes-protsesiv, yikh optymizatsiia* [Digitization – as a tool for improving business processes, optimizing them]. *Ekonomika. Menedzhment. Biznes* [Economy. Management. Business], *1 (23)*, 33-39 [in Ukrainian].
9. *Postanova Pytannia Yedynoho derzhavnoho vebportalu elektronnykh posluh ta Reiestru administratyvnykh posluh, 2019* (Kabinet Ministriv Ukrainy) [Resolution Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services, 2019 (Cabinet of Ministers of Ukraine)]. *Ofitsiinyi sait Verkhovnoji Rady Ukrajiny* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text> (2022, November, 07) [in Ukrainian].
10. Eufordigital.eu (2020). *EU4Digital: supporting digital economy and society in the Eastern Partnership Cybersecurity guidelines for the Eastern Partner countries* <https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf> (2022, November, 11). [in Ukrainian].
11. *Zakon Ukrainy Pro krytychnu infrastrukturu, 2021* (Verkhovna Rada Ukrainy) [Law of Ukraine On Critical Infrastructure, 2021 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoji Rady Ukrajiny* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (2022, November, 11). [in Ukrainian].
12. Ministerstvo ta Komitet tsyfrovoi transformatsii Ukrainy [Ministry and Committee of Digital Transformation of Ukraine] (2021). *The Ukrainian IT Sector: An Overview of Publicly Available Data and Gaps in Market* <https://drive.google.com/file/d/1hgoJ5n553xJbi6n6X0wwR9sRJWzdMiFU/view> (2022, November, 25).
13. *Postanova Polozhennia pro zakhyst informatsii ta kiberzakhyst uchasnykamy platizhnoho rynku, 2021* (Natsionalny Bank Ukrainy) [Resolution Regulation on Information Protection and Cyber Defense by Payment Market Participants, 2021 (National Bank of Ukraine)]. *Ofitsiinyi sait Verkhovnoji Rady Ukrajiny* [Official website

of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/v0043500-21#Text> (2022, November, 21). [in Ukrainian].
14. *Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, 2017* (Verkhovna Rada Ukrainy) [Resolution of the National Bank of Ukraine Regulation on Information Protection and Cyber Defense by Payment Market Participants, 2017 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoji Rady Ukrajiny* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (2022, November, 21). [in Ukrainian].
15. *Zakon Ukrainy Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo zabezpechennia ukladennia uhody mizh Ukrainoiu ta Yevropeiskym Soiuzom pro vzaiemne vyznannia kvalifikovanykh elektronnykh dovirchykh posluh ta implementatsii zakonodavstva Yevropeiskoho Soiuzu u sferi elektronnoi identyfikatsii, 2022* (Verkhovna Rada Ukrainy) [Law of Ukraine On Amendments to Certain Legislative Acts of Ukraine to Ensure the Conclusion of an Agreement between Ukraine and the European Union on Mutual Recognition of Qualified Electronic Trust Services and the Implementation of European Union Legislation in the Field of Electronic Identification, 2022 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoji Rady Ukrajiny* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/2801-20#Text> (2022, November, 24). [in Ukrainian].
16. *Postanova Pro realizatsiiu eksperymentalnoho proektu iz stvorennia, vprovadzhennia ta zabezpechennia funktsionuvannia Yedynoi tsyfrovoi intehrovanoi informatsiino-analitychnoi systemy upravlinnia protsesom vidbudovy infrastruktury, 2022* (Kabinet Ministriv Ukrainy) [Resolution On the Implementation of a Pilot Project for the Creation, Implementation and Operation of the Unified Digital Integrated Information and Analytical System for Managing the Infrastructure Reconstruction Process, 2022 (Cabinet of Ministers of Ukraine)]. *Ofitsiinyi sait Verkhovnoji Rady Ukrajiny* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/1286-2022-%D0%BF#Text> (2022, November, 18). [in Ukrainian].
17. *Postanova Polozhennia Pro zatverdzhennia Polozhennia pro orhanizatsiiu kiberzakhystu v bankivskii systemi Ukrainy ta vnesennia zmin do Polozhennia pro vyznachennia obiektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy, 2022* (Natsionalnyi bank Ukrainy) [Resolution Regulation On Approval of the Regulation on the Organization of Cyber Defense in the Banking System of Ukraine and Amendments to the Regulation on the Definition of Critical Infrastructure Objects in the Banking System of Ukraine, 2022 (National Bank of Ukraine)]. *Ofitsiinyi sait Natsionalnoho banku Ukrainy* [Official website of the National Bank of Ukraine] <https://bank.gov.ua/ua/legislation/Resolution_12082022_178> (2022, November, 19). [in Ukrainian].
18. *Postanova Pro zatverdzhennia Poriadku vykorystannia koshtiv z rakhunka Ministerstva tsyfrovoi transformatsii dlia zabezpechennia protydii informatsiinym zahrozam z boku derzhavy-ahresora, kiberzakhystu, vidnovlennia ta rozvytku tsyfrovoi infrastruktury derzhavy, 2022* (Kabinet Ministriv Ukrainy) [Resolution On Approval of the Procedure for the Use of Funds from the Account of the Ministry of Digital Transformation to Ensure Counteraction to Information Threats from the Aggressor State, Cyber Defense, Restoration and Development of the State's Digital Infrastructure, 2022 (Cabinet of Ministers of Ukraine)]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official website of the National Bank of Ukraine] <https://zakon.rada.gov.ua/laws/show/751-2022-%D0%BF#Text> (2022, November, 27). [in Ukrainian].
19. *Zakon Ukrainy Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zabezpechennia funktsionuvannia informatsiino-komunikatsiinykh system, elektronnykh komunikatsiinykh system, publichnykh elektronnykh reiestriv, 2022* (Verkhovna Rada Ukrainy) [Law of Ukraine On Amendments to Certain Laws of Ukraine on Ensuring the Functioning of Information and Communication Systems, Electronic Communication Systems, Public Electronic Registers, 2022 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/2130-20#Text> (2022, November, 29). [in Ukrainian].
20. *Zakon Ukrainy Pro khmarni posluhy, 2022* (Verkhovna Rada Ukrainy) [Law of Ukraine On Cloud Services, 2022 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy.* [Official website of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text> (2022, November, 18). [in Ukrainian].