

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2022. № 10.

DOI: <http://doi.org/10.32702/2307-2105.2022.10.40>

УДК 338.16+658.310

Т. В. Капелюшина,

к. е. н., доцент, доцент кафедри управління інформаційною та кібернетичною безпекою, Державний університет телекомунікацій

ORCID ID: <https://orcid.org/0000-0001-7490-6751>

РОЗШИРЕННЯ БАЗОВИХ СКЛАДОВИХ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА З УРАХУВАННЯМ УМОВ НЕВИЗНАЧЕНОСТІ

T. Kapeliushna,

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

EXPANDING THE MAIN COMPONENTS OF ECONOMIC SECURITY OF ENTERPRISE, TAKING INTO ACCOUNT THE CONDITIONS OF UNCERTAINTY

У статті досліджено теперішні умови невизначеності та розглянуто питання важливості безпеки секторів інфраструктури, що слугують підґрунтям для економічної безпеки макрорівня та підприємств. Окреслено складові економічної безпеки підприємств з урахуваннях несприятливих умов та змін, що ними спричиняються, підкреслено важливість інфокомунікацій як складової економічної безпеки підприємства, оскільки господарючі суб'єкти нині, не залежно від того, яку діяльність вони провадять, намагаються функціонувати, що уможлиблюється в умовах невизначеності саме за рахунок електронних послуг, що надаються операторами та провайдерами зв'язку.

Відзначено, що доповнення складової безпеки - електронно-комунікаційною (з урахуванням введення в дію ЗУ «Про електронні комунікації»), дозволить в теперішніх невизначених умовах удосконалити оцінювання економічної безпеки підприємства та враховувати результати оцінки при розробці заходів, інструментів, механізмів управління економічною безпекою підприємства.

The article investigates the current conditions of uncertainty and considers the importance of security of critical infrastructure sectors (which include the information technology sector and the electronic communications sector), which serve as the basis for economic security at all levels: macro-level - mesolevel - enterprise. Outlined the components of the economic security of enterprises, taking into account adverse conditions and changes that they cause, stressed the importance of infocommunications as a component of the economic security of the enterprise, because business entities are now, regardless of what activities they perform, trying to function, which is made possible in conditions of uncertainty due to the electronic services provided by operators and communications providers.

It describes the new possibilities of communication that appear with the introduction of the next generations of mobile standards (4 G, 5G, 6 G) and the approach of society to the digitalization of the world and the new standards of economic security. It is emphasized that digital business today is changing and adapting to new conditions and requires a new approach to remote access: detailed security; global scalability; optimized performance. It is noted that the technologies of remote Internet access are changing, so the VPN technology is replaced by Zero Trust Network Access, a network access with zero trust, which provides secure access to modern business. Analyzed (according to the World Bank), the security of Internet servers in countries around the world and the conclusion that Ukraine gravitates to solving the issues of protection and safety, implementing new laws and regulations, regulations, global standards, which protect businesses in the info-communication space.

It is noted that the addition of the component of security - electronic communications (taking into account the introduction of the Law of Ukraine "On electronic communications"), will improve the assessment of economic security of the enterprise in the current uncertain conditions and take into account the results of the assessment when developing measures, tools, mechanisms of economic security management of the enterprise.

Ключові слова: складові економічної безпеки, електронно-комунікаційна складова, електронні комунікації, економічна безпека підприємства, сектор критичної інфраструктури, безпечність серверів, невизначені умови, обставини непереборної сили

Keywords: economic security components, electronic communications component, electronic communications, economic security of the enterprise, critical infrastructure sector, server security, uncertain conditions, force majeure

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В умовах невизначеності та глобальних проблем людства, таких як: пандемія, що спричинена поширенням коронавірусної хвороби, проблеми зміни клімату, війни, недостатня забезпеченість продовольчими товарами та енергоносіями у деяких країнах світу, відсутність послуг зв'язку, освітніх послуг призводять до актуалізації питань «економічної безпеки». Питання стосуються й базового соціального забезпечення, котрі визначаються рівнем доступу до інфраструктури (в сфері транспорту, зв'язку, освіти, здоров'я, безпеки). Звісно ж, аналогічні питання торкаються й суб'єктів господарювання, особливо гостро питання економічної безпеки підприємств постає в обставинах непереборної сили, до яких відносять і воєнний стан в Україні. Будь-яке підприємство, бізнес-структура має дбати належним чином про економічну безпеку, щоб виконувати свою функцію – задовольняти потреби споживачів та отримувати прибуток, а для держави виступати як економічна одиниця, яка забезпечує виконання своїх функцій та поповнювати бюджет. Саме вивчення складових економічної безпеки з урахуванням несприятливих умов та змін, що ними спричиняються, можуть стати у нагоді при формуванні механізмів та розробці комплексних заходів щодо усунення загроз та забезпеченні економічної безпеки підприємства, чим і актуалізується питання для дослідження.

Аналіз останніх досліджень та публікацій. Вивченню складових економічної безпеки підприємства присвячені наукові праці вчених: Ю. Работіна, В. Вороніної, Т. Меліхової, Б. Буркинського та В. Грищенко, С. Ілляшенко, Е. Данілової, Б. Дуб, С. Покропивного, В. Геєця [6; 7; 8; 9; 10; 18; 11;

12; 13], однак невизначені умови, що виникають впродовж останніх трьох років потребують розширення переліку складників з урахуванням посилення ролі електронних послуг, цифровізації економіки та діджиталізації суспільства в період пандемії та воєнного стану в країні. У напрямку розгляду питання – важливості послуг телекомунікаційної сфери у функціонуванні та безпеці підприємств, проведено низку досліджень вченими: О. Гудзь, Л. Худолій, С. Легоміною, В. Сотниченком, О. Сосновською, В. Пильною [14; 15; 16; 17], які слугуватимуть базисом для проведення аналізу та обґрунтування важливості інфокомунікацій як складової економічної безпеки підприємства.

Формулювання цілей статті. Розширити перелік складових економічної безпеки підприємства - електронно-комунікаційною, з урахуванням посилення ролі електронної комунікації в нинішніх умовах невизначеності, що дозволить в даних умовах удосконалити оцінювання економічної безпеки підприємства та враховувати результати оцінки при розробці заходів, інструментів, механізмів управління економічною безпекою підприємства.

Виклад основного матеріалу дослідження. Із плином часу та розвитком економіки та суспільства поняття «економічна безпека підприємства» переходить у новий формат, який включатиме інформатизацію та цифровізацію економічних процесів в складниках, які враховуються при формуванні механізму управління економічною безпекою підприємства. Телекомунікації при цьому відіграють особливу роль, оскільки забезпечують безперебійне функціонування господарюючих суб'єктів в умовах невизначеності, як спостерігалось в період запровадження локдауну при поширенні коронавірусної хвороби, так і під час воєнного стану. Галузь зв'язку слугує невід'ємним компонентом у діяльності всіх підприємств, крім того, визначається критично важливим сектор, оскільки забезпечує допоміжну функцію у всіх секторах інфраструктури, в тому числі - критично важливих.

Інформаційні технології виокремлено як один із 16 критично важливих секторів критичною інфраструктури, що підтверджується директивою RPD-21 [4]. За Законом України «Про критичну інфраструктуру» [1] серед критично

важливих послуг - інформаційні послуги та електронні комунікації. У переліку секторів (підсекторів), основних послуг критичної інфраструктури країни знаходиться й інформаційний сектор, який містить:

1) підсектор інформаційних технологій, який включає в себе:

- надання хмарних послуг, у тому числі зберігання та обробки даних у центрах обробки даних та/або хмарних сховищах, здійснення хмарних обчислень;
- забезпечення функціонування систем електронного урядування;
- розповсюдження ефірного цифрового наземного мовлення з використанням радіочастотного спектра в трьох та більше областях країни.

2) підсектор електронні комунікації, який включає в себе:

- забезпечення функціонування точок обміну Інтернет-трафіком (IXP);
- адміністрування адресного простору українського сегмента Інтернету, у тому числі надання послуг з підтримки та адміністрування систем доменних імен (DNS) в Інтернеті;
- адміністрування та ведення реєстрів доменних імен верхнього рівня в Інтернеті, у тому числі домену «.UA».

Галузь зв'язку нині представляє собою конкурентоздатну, взаємопов'язану галузь, що поєднує та використовує наземні, супутникові та бездротові системи передачі даних, між собою пов'язані провайдери дротової, супутникової та бездротової мережі, наразі вони залежні один від одного в частині передавання та термінації трафіку, компанії часто спільно використовують засоби та технології для забезпечення відповідності та можливості якісного та безперебійного надання по телекомунікаційних послуг.

Однозначно, що господарюючі суб'єкти нині, не залежно від того, яку діяльність вони провадять, намагаються виконувати свої функції та

функціонувати, що уможлиблюється в умовах невизначеності саме за рахунок електронних послуг, що надаються операторами та провайдерами зв'язку.

Слід підкреслити важливість еволюції інформаційно-комунікаційних технологій, які продовжують забезпечувати високий рівень взаємопов'язаних та цифрових й електронних операцій в межах безпеки на всіх рівнях: мікробезпеки (підприємства), мезобезпеки (регіонів), макробезпеки (держави). На сьогодні вже йдеться про шосте покоління мобільного зв'язку - 6 G, завдяки його появі суттєво розширяться можливості його використання, а також реалізуються програми, що націлені на цифровізацію суспільства (порівняння стандартів мобільного зв'язку 4 G, 5 G, 6 G наведено на рис. 1)



Рис. 1. Нові можливості зв'язку із впровадженням наступних поколінь стандартів мобільного зв'язку

Джерело: складено автором за даними ITU [20]

Зрозуміло, що стандарти 5 G розширюють можливості підприємств, що їх використовують, оскільки підвищується надійність зв'язку, а отже й

стабільність передачі даних, зменшується кількість відмов при передачі даних, збільшується кількість підключень гаджетів.

Поява та використання нового стандарту Generation 6 (G 6) дозволить реалізувати цифровізацію у всіх сферах, автоматизувати зв'язок та створити розумні міста.

Зрозуміло, що нові стандарти наближують суспільство до цифровізації світу, використання їх дозволить підприємствах посилити економічну безпеку у частині обробки інформації, а отже й інформаційної складової за рахунок саме інноваційних технологій.

Сьогодення потребує перелаштування на віддалений доступ, який став основною вимогою для підприємств незалежно від виду діяльності, який ним провадиться, його розмірів. Здатність підприємства миттєво, безпечно та в повною мірою перейти до моделі «робота з будь-якого місця» визначатиме, як воно переживе невизначені умови, які переводять нас у режим віддаленої роботи, а підприємства у онлайн функціонування.

Саме тому, сучасний цифровий бізнес сьогодні змінюється та адаптується до нових умов і потребує нового підходу щодо віддаленого доступу: деталізованої безпеки; глобальної масштабованості; оптимізованої продуктивності. Змінюються технології забезпечення віддаленого доступу в Інтернет, так технологію VPN замінює Zero Trust Network Access – мережевий доступ з нульовою довірою, який забезпечує надання безпечного доступу до сучасного бізнесу. За надання через хмарну службу SDP усуває обмеження масштабованості VPN й миттєво забезпечує збільшення віддаленого доступу без необхідності додаткового обладнання або програмного забезпечення. SDP також забезпечує підвищену безпеку, оскільки забезпечує детальний контроль доступу на рівні додатків, а також можливості моніторингу.

Отже, прослідковуються зміни у бік діджиталізації та цифровізації світу, тому слід урахувати посилення ролі та значення інфокомунікацій та електронних комунікацій у функціонуванні економічних одиниць будь-якої сфери, тому стає доцільним розглянути їх у розрізі економічної безпеки підприємств, зокрема її складових.

Вивченню складових економічної безпеки підприємства присвячені наукові праці вчених: Ю. Работіна, В. Вороніної, Т. Меліхової, Б. Буркинського та В. Грищенко, С. Ілляшенко, Е. Данілової, С. Покропивного, В. Геєця [6; 7; 8; 9; 10; 18; 11; 12; 13].

Базовими складовими економічної безпеки підприємства вважаються за думкою науковців:

- фінансова, яка вбачається у забезпеченні безпечного руху коштів, а також стійкого фінансового стану;
- техніко-технологічна, що окреслює умови безпеки к використання матеріальної та технічної бази;
- виробнича – включає забезпечення виконання функцій операційної діяльності;
- енергетична – передбачає заходи для максимальної економії енергоносіїв;
- політико-правова – врахування всіх норм, правил, законів та положень, що регулюють діяльність сфери, в якій функціонує підприємство;
- ринкова – відповідність умовам ринку, конкурентоспроможність продукції та її якість відповідно до вимог ринку;
- інтелектуальна та кадрова, яка відповідає за безпечні умови роботи персоналу, захист їх прав та правомірне використання їх інтелектуального потенціалу;
- інтерфейсна, яка характеризується надійністю взаємодії з економічними контрагентами (споживачами, конкурентами, постачальниками, кредиторами, посередниками).;
- інформаційна – у системі захисту комерційної таємниці, збереженні цілісності та достовірності даних;
- силова представляє собою фізичний захист як приміщень, так і персоналу та інформації, а також матеріальних об'єктів підприємства;
- екологічна – через політику захисту навколишнього середовища.

Такий підхід є безперечно правильним, але з урахуванням плину часу та невизначених умов, що виникають впродовж останніх трьох років потребує

розширення переліку складових з урахуванням посилення ролі електронних послуг, цифровізації економіки та діджиталізації суспільства в період пандемії та воєнного стану в країні. У напрямку розгляду даного питання – важливості послуг телекомунікаційної сфери у функціонування та безпеці підприємств, проведено низку досліджень вченими: О. Гудзь, Л. Худолій, С. Легоміною, В. Сотниченком, О. Сосновською, В. Пильною [14; 15; 16; 17]. Зокрема, О. Сосновською [15] підкреслюється динамічний розвиток телекомунікаційної сфери серед галузей світової економіки, а також суттєвий вплив на функціонування підприємств, соціально-економічний розвиток регіонів. Тому науковицею пропонується інноваційно-інформаційна складова економічної безпеки, що є цілком доцільно до розгляду в умовах цифровізації суспільства.

З причин невизначеності умов (особливо з часів поширення Covid-19) безпека у інформаційному та телекомунікаційному просторі набуває особливої значимості, світовими організаціями проводяться дослідження та наводяться статистичні дані безпечності роботи у глобальній мережі. Світовим банком проводився аналіз у розрізі країн світу щодо безпечності інтернет-серверів, найбільш безпечними вважаються сервери Сполучених Штатів Америки - 46678110 серверів на 1 млн. осіб, потім – Німеччини 8109646 серверів на 1 млн. осіб й Великої Британії - 2445275 серверів на 1 млн. осіб. Щодо України, то показник відчутно нижчий - 395092 сервери на 1 млн. осіб (рис. 2).

Зрозуміло, що розвиток техніки та технологій, інфокомунікацій, поширення Інтернет у досліджуваних країнах відбувався швидшими темпами. Крім того, з появою глобальної мережі та інтернет-технологій у досліджуваних країнах (що займають лідируючі позиції захисту серверів) з'являлися послуги, що надавалися за їх використання, тому й питання захисту та безпеки в інфокомунікаційному просторі ставилися одночасно із їх наданням. Саме тому рівень захисту та безпеки у даних країнах в цифровому просторі вище. Україна тяжіє до вирішення питань захисту та безпеки, імплементує нові закони та положення, нормативно правові-акти, світові стандарти, які убезпечують роботу підприємств у інфокомунікаційному просторі.

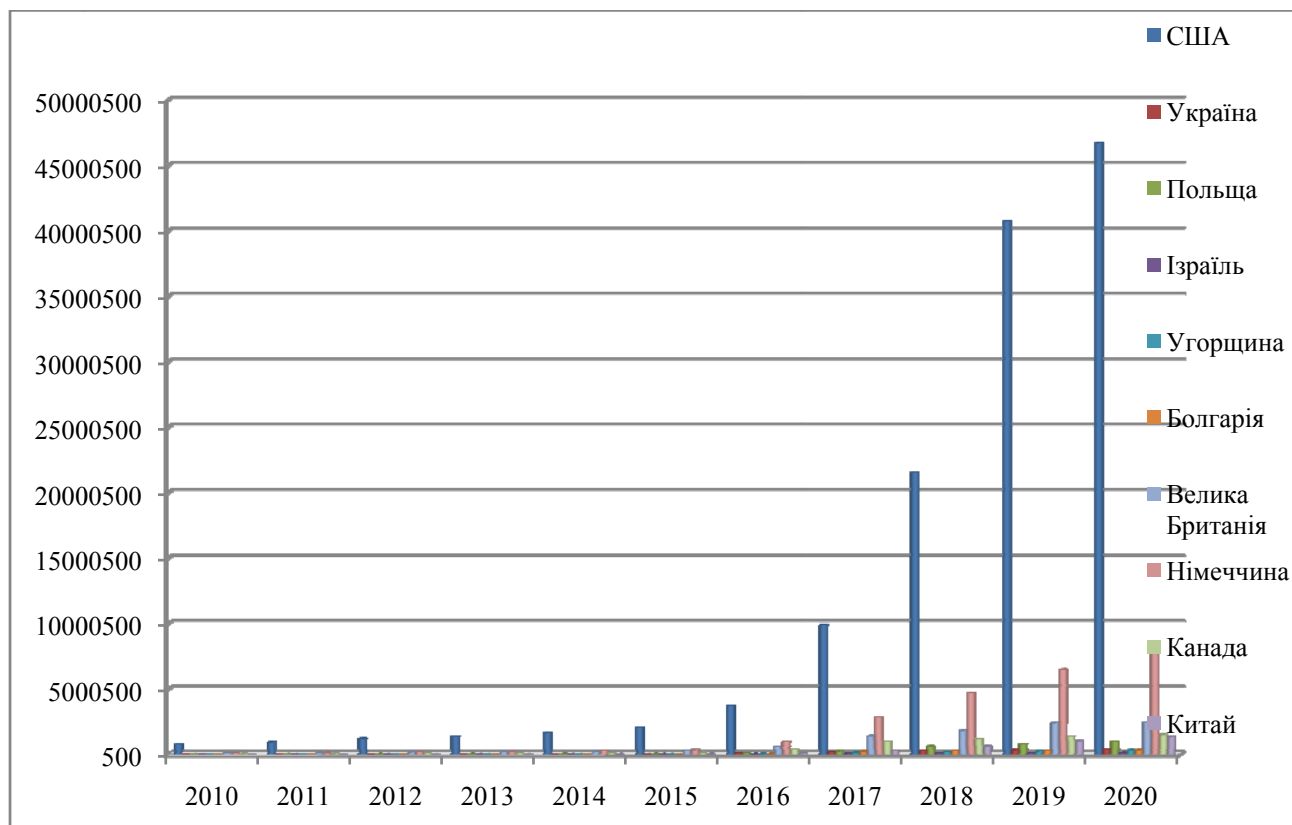


Рис. 2. Динаміка показників безпечності інтернет-серверів (на 1 млн. осіб) за країнами світу впродовж 2010-2020 рр.

Джерело: складено автором на основі даних The World Bank [19]

Стали доступними мережі 4G, імплементуються акти Європейського Союзу, щодо управлінням радіочастотного спектра. Наприкінці 2019 року Європейський Союз офіційно розпочав в Україні нову програму «EU4Digital: підтримка цифрової економіки та суспільства у Східному партнерстві». Дана програма передбачає розширити переваги Єдиного цифрового ринку Європейського Союзу для України та інших держав Східного партнерства з метою стимулювання економічного росту, створення робочих місць, покращення життя людей та допомоги бізнесу.

Тому в Україні на законодавчому рівні зазнають змін правила, що регулюють діяльність у сфері телекомунікацій. Так, втратив чинність ЗУ «Про телекомунікації» (якому передував ЗУ «Про зв'язок»), замість нього у 2022 році введено в дію Закон України «Про електронні комунікації» [1], зміна якого пояснюється динамічним розвитком сфери та важливістю регулювання підприємств, що функціонують у телекомунікаційній сфері у відповідності до

нових умов та світових вимог до підприємств зв'язку та послуг, що ними надаються.

Даним законом «електронна комунікація» визначається як: передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій; а «електронна комунікаційна послуга» - як послуга, що полягає в прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг. Сутність даних категорій та їх смислове значення, дозволяє прийти до висновку, що на сьогодні будь-яке підприємство, враховуючи умови невизначеності (що спричиняються загрозами, на які безпосередньо вплинути не може, а може лише адаптуватися), продовжує функціонувати лише шляхом електронної комунікації. Саме тому, крім перерахованих вище складових (фінансової, техніко-технологічної, виробничої, енергетичної, ринкової, інтелектуальної, кадрової, інтерфейсної, інформаційної, силової, політико-правової, екологічної, інформаційно-інноваційної) доцільно ввести електронно-комунікаційну. У свою чергу включення даної складової до базових дозволить суттєво посилити економічну безпеку підприємств, оскільки дозволить розширити врахування ризиків з метою подальшого вивчення та уникнення переходу їх у загрози економічній безпеці підприємства. Особливо відчутна важливість електронної комунікації для підприємств в умовах воєнного стану, оскільки деяким підприємствам довелося змінити формат провадження своєї діяльності й своє територіальне місцезнаходження. Слід розуміти, що введена складова дозволить покращити процес оцінки економічної безпеки та визначати її рівень.

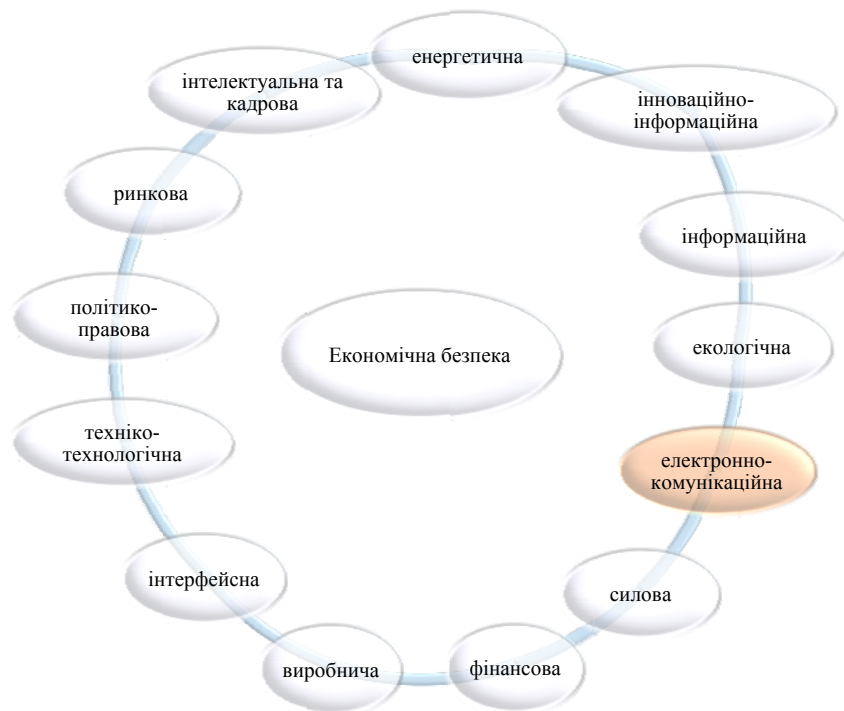


Рис. 3. Складові економічної безпеки підприємства з урахуванням посилення ролі електронних послуг в умовах невизначеності (авторське доповнення)

Джерело: узагальнено автором на основі [7-13;15]

Розширення складових (з урахуванням умов невизначеності та потреби здійснювати левову частку роботи віддалено) дозволить якісніше та повною мірою охопити можливі ризики, виклики та загрози, оцінити показники рівнів впливу кожної із складових, визначити вагомість окремої складової економічної безпеки здійснити та провести інтегральну оцінку економічної безпеки.

Висновки та перспективи подальших розвідок у даному напрямі. Отже, аналіз і оцінювання рівнів складових економічної безпеки є основою для розроблення комплексу заходів протидії загрозам та підвищення рівня економічної безпеки підприємства і, відповідно, розширення його адаптаційних можливостей до змін умов господарської діяльності, створення умов стабільного функціонування і розвитку.

Крім того, доцільність перегляду складових економічної безпеки підприємства з урахуванням мінливості середовища, умов функціонування та невизначеностей має сенс через те, що її рівень визначається у послідовності:

Оцінювання кожної складової економічної безпеки підприємства, що досліджується;

Визначення вагомості кожної складової економічної безпеки досліджуваного підприємства

Отже, визначення рівня економічної безпеки підприємства розпочинається саме з оцінки складових економічної безпеки, тобто не врахувавши або обравши їх неправильно унеможлиблюється достовірність та правильність визначення рівня економічної безпеки для досліджуваного підприємства.

Саме за рахунок постійного моніторингу змін, що виникають під дією зовнішнього оточення та факторів впливу, вдасться більш досконало проводити аналіз та оцінку складових економічної безпеки, ранжувати їх за ступенем сили дії з подальшою розробкою алгоритму виявлення ризиків, що можуть перейти у виклики та спричинити загрозу економічній безпеці підприємства. Далі розробити комплекс заходів щодо нейтралізації виявлених загроз та адаптувати до несприятливих умов, забезпечити стабільне, безпечне функціонування підприємства та сприяти його розвитку, розкриттю потенційних можливостей. Пропозиція доповнення складової безпеки - електронно-комунікаційною, дозволить в теперішніх невизначених умовах удосконалити оцінювання економічної безпеки підприємства та враховувати результати оцінки при розробці заходів, інструментів, механізмів управління економічною безпекою підприємства.

Література

1. Верховна Рада України: офіційний веб-сайт. Закон України від 16.11.2021 № 1882-IX «Про критичну інфраструктуру» URL:: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (Дата звернення: 07.09.2022).

2. Верховна Рада України: офіційний веб-сайт. Постанова Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури: порядок, перелік, методика». URL:: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42>. (Дата звернення: 08.09.2022).

3. Верховна Рада України: офіційний веб-сайт. Закон України від 16.12.2020 № 1089-IX «Про електронні комунікації». URL: <https://zakon.rada.gov.ua/laws/show/1089-20/sp:max50:nav7:font2#Text> (Дата звернення: 10.09.2022).

4. The White House. Directive PPD-21. URL: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (Дата звернення: 11.09.2022).

5. Rosenstein-Rodan, P.N. (1961). The Notes of the Theory of the “Big Bush” in Economic Development for Latin America. London, New York.

6. Rabotin, Y. (n.d.). (2022). “The Essence of economic Security and the Principles of its Provision at the Enterprise”. *Revista Română de Statistică – Supliment*, vol. 8, pp. 37-42.

7. Voronina, V. (n.d.). Economic Security of Enterprises: the Essence, Factors of Influence, and Methods of Protection. Security Of The Xxi Century: National And Geopolitical Aspects: collective monograph. Prague: Nemoros s.r.o., 2019. pp. 217-223.

8. Melikhova, T. (2020) Analysis of available Methods for Assessing the Level of Economic Security of an Enterprise for Conducting Modern Diagnostics of its Financial Condition. *Innovative Economy*, vol. 1-2, pp. 223-227.

9. Burkynskyi, B., & Gryshchenko, V. (2020). Factors Of Ensuring Economic Security In The Process Of Innovative Development Of Entrepreneurship. *Economic Innovations*, vol. 22(3(76)), pp. 6-29.

10. Ілляшенко, О.В. Механізм функціонування системи економічної безпеки підприємства: підхід до побудови. *Економіка. Менеджмент. Підприємництво*. 2014. No 26(1). С. 160-168.

11. Дуб Б.С. Система економічної безпеки підприємства: поняття та структура. *Управління проектами та розвиток виробництва*. 2016. №4(60.) С. 5-9. URL: https://www.researchgate.net/publication/322958986_Sistema_ekonomichnoi_bezpeki_pidpriemstva_ponatta_ta_struktura (дата звернення: 11.10.2022)

12. Покропивний С.Ф. Економіка підприємства. К.: КНЕУ, 2000. 526 с.

13. Геєць В.М. Моделювання економічної безпеки: держава, регіон, підприємство. Х.: ВД «ІНЖЕК». 2006. 240 с.
14. Гудзь О. Є., Сотниченко В.М. Принципи та умови забезпечення економічної безпеки телекомунікаційних підприємств. *Економіка. Менеджмент. Бізнес*. 2016. № 4. С. 12-19. URL: http://nbuv.gov.ua/UJRN/естебі_2016_4_4 (дата звернення: 17.09.2022)
15. Сосновська О. О. Методичний підхід до оцінки рівня економічної безпеки підприємств зв'язку. *Облік і фінанси*. 2019. № 1. С. 168-176. URL: http://nbuv.gov.ua/UJRN/Oif_apk_2019_1_22 (дата звернення: 18.09.2022)
16. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3. С. 87-92. URL: http://nbuv.gov.ua/UJRN/естебі_2015_3_18 (дата звернення: 18.09.2022)
17. Пильнова В.П., Капелюшна Т.В., Овсійчук В.Я., Красник О.А. Місце інноваційних ризиків у системі економічної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2021. № (4). С. 61-68.
18. Данілова Е. І. Концепція системного підходу до управління економічною безпекою підприємства: монографія. Вінниця: Європейська наукова платформа, 2020. 342 с.
19. Secure Internet Servers. The World Bank. URL: <https://data.worldbank.org/indicator/IT.NET.SECR?end=2020&start=2010&type=shaded&view=map&year=2020> [accessed Oct 15 2022].
20. The official web-site of ITU (2022). “5G - Fifth generation of mobile technologies”. URL: <https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx> (accessed Oct 9 2022).

References

1. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine “About critical infrastructure”, available at: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (Accessed 07 September 2022)
2. Cabinet of Ministers of Ukraine (2020), Resolution “Some issues of critical infrastructure objects: order, list, methodology”, available at: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (Accessed 08 September 2022)

3. The Verkhovna Rada of Ukraine (2020), The Law of Ukraine “About electronic communications”, available at: <https://zakon.rada.gov.ua/laws/show/1089-20/sp:max50:nav7:font2#Text> (Accessed 10 September 2022)

4. The White House (2013), “Directive PPD-21”, available at: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (Accessed 11 September 2022)

5. Rosenstein-Rodan, P.N. (1961), The Notes of the Theory of the “Big Bush” in Economic Development for Latin America, London, New York.

6. Rabotin, Y. (2022), “The Essence of economic Security and the Principles of its Provision at the Enterprise”, *Revista Română de Statistică – Supliment*, vol. 8, pp. 37-42.

7. Voronina, V. (2019), “Economic Security of Enterprises: the Essence, Factors of Influence, and Methods of Protection”, *Security Of The Xxi Century: National And Geopolitical Aspects: collective monograph*, Prague, Czech Republic, pp. 217-223.

8. Melikhova, T. (2020), “Analysis of available Methods for Assessing the Level of Economic Security of an Enterprise for Conducting Modern Diagnostics of its Financial Condition”, *Innovative Economy*, vol. 1-2, pp. 223-227.

9. Burkynskyi, B. and Gryshchenko, V. (2020), “Factors Of Ensuring Economic Security In The Process Of Innovative Development Of Entrepreneurship”, *Economic Innovations*, vol. 22(3(76)), pp. 6-29.

10. Illiashenko, O.V. (2014), “Mechanism of functioning of the economic security system of the enterprise: approach to construction”, *Ekonomika. Menedzhment. Biznes*, vol 26 (№1), pp. 160-168.

11. Dub, B (2016), ”System of economic security of the enterprise: concept and structure”, *Upravlinnia proektamy ta rozvytok vyrobnytstva*, [Online], vol. 4(60), pp. 5-9, available at: https://www.researchgate.net/publication/322958986_Sistema_ekonomicnoi_bezpeki_pidpriemstva_ponatta_ta_struktura (Accessed Oct 11 2022)

12. Pokropyvnyi, S.F. (2000), *Ekonomika pidpriemstva* [The economy of the enterprise], KNEU, Kyiv, Ukraine.

13. Heiets, V.M. (2006), *Modeliuvannia ekonomichnoi bezpeky: derzhava, rehion, pidpriemstvo* [Modeling of economic security: state, region, enterprise], VD «INZhEK», Kharkiv, Ukraine.

14. Hudz, O. Ye. and Sotnychenko, V.M. (2016), “Principles and conditions for ensuring the economic security of telecommunications enterprises”, *Ekonomika. Menedzhment. Biznes*, vol. 4, pp. 12-19, available at: http://nbuv.gov.ua/UJRN/ecmebi_2016_4_4 (Accessed 17 September 2022)

15. Sosnovska, O. O. (2019), “A methodical approach to assessing the level of economic security of communication enterprises”, *Oblik i finansy*, vol. 1, pp. 168-179, available at: http://nbuv.gov.ua/UJRN/Oif_apk_2019_1_22 (Accessed 18 September 2022)/

16. Lehominova, S. V. (2015), “Theoretical principles of enterprise information security”, *Ekonomika. Menedzhment. Biznes*, vol. 3, pp. 87-92, available at: http://nbuv.gov.ua/UJRN/ecmebi_2015_3_18 (Accessed 18 September 2022)

17. Pylnova, V.P. and Kapeliushna, T.V. (2021), “The place of innovative risks in the system of economic security of the enterprise”, *Ekonomika. Menedzhment. Biznes*, vol. 4, pp. 61-68.

18. Danilova, E. I. (2020), *Kontseptsiiia systemnoho pidkhodu do upravlinnia ekonomichnoiu bezpekoiu pidpriemstva* [The concept of a systematic approach to the management of the economic security of the enterprise], Yevropeiska naukova platform, Vinnytsia, Ukraine.

19. The World Bank (2020), “Secure Internet Servers”, available at: <https://data.worldbank.org/indicator/IT.NET.SECR?end=2020&start=2010&type=shaded&view=map&year=2020> (Accessed Oct 15 2022).

20. The official web-site of ITU (2022), “5G - Fifth generation of mobile technologies”, available at: <https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx> (Accessed Oct 9 2022).

Стаття надійшла до редакції 20.10.2022 р.