УДК 330.341.1: 316.42
JEL Classification: L86

# НАУКОВО-МЕТОДИЧНІ ЗАСАДИ ОЦІНКИ ЕФЕКТИВНОСТІ ПРОЦЕСУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ: КІБЕРБЕЗПЕКА ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ

©2022 **БОНДАР-ПІДГУРСЬКА О. В., ХОМЕНКО І. І.**

*УДК 330.341.1: 316.42*
*JEL Classification: L86*

**Бондар-Підгурська О. В., Хоменко І. І.**

**Науково-методичні засади оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу: кібербезпека та інтелектуальна власність**

*Метою статті є дослідження науково-методичних засад оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу та розробка рекомендацій щодо підвищення його ефективності в умовах зростання викликів і загроз їх кібербезпеці та інтелектуальній власності. При цьому основними методами дослідження стали: аналіз, синтез, узагальнення, табличні, графічні, а також комплексний підхід. Актуалізовано важливість і необхідність своєчасної оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу через зростання кіберзагроз їх інтелектуальній власності як основи інноваційного розвитку в умовах пандемії, війни, діждиталізації. Обґрунтовано процес управління інформаційною безпекою щодо захисту об'єктів інтелектуальної власності (ОІВ) як надійне підґрунтя для забезпечення інноваційного розвитку підприємств малого та середнього бізнесу. При цьому наголошено на зростанні важливості, ролі та значущості кібербезпеки для функціонування та розвитку підприємств малого та середнього бізнесу в умовах нових викликів і загроз. Розроблено та запропоновано до використання науково-методичний підхід щодо оцінки ефективності процесу управління інформаційною безпекою в контексті захисту ОІВ підприємств малого та середнього бізнесу в умовах зростаючої кількості викликів і загроз. Наголошено на доцільності детального дослідження напрямів удосконалення нормативно-законодавчої бази з питань інформаційної безпеки щодо захисту ОІВ підприємств малого і середнього бізнесу в умовах протистояння кіберзагрозам. Висвітлено перспективні напрями досліджень цієї проблематики: розробка стратегії інформаційної безпеки щодо захисту ОІВ у контексті попередження нових викликів і загроз; удосконалення організаційних аспектів управління інформаційною безпекою щодо захисту ОІВ; розвиток цифрової культури підприємств малого та середнього бізнесу як чинника підвищення ефективності процесу управління інформаційною безпекою в умовах викликів діджиталізації.*

***Ключові слова:*** *інформаційна безпека, підприємства малого та середнього бізнесу, кібербезпека, інтелектуальна власність, оцінки ефективності, процес управління.*

***DOI:*** *https://doi.org/10.32983/2222-0712-2022-2-108-116*

***Рис.:*** *4.* ***Табл.:*** *1.* ***Бібл.:*** *15.*

***Бондар-Підгурська Оксана Василівна*** *– доктор економічних наук, доцент, доцент кафедри менеджменту, Полтавський університет економіки і торгівлі (вул. Коваля, 3, Полтава, 36014, Україна)*

***E-mail:*** *Bondarpodgurskaa@gmail.com*

***ORCID:*** *http://orcid.org/0000-0001-7792-4023*

***Researcher ID:*** *https://publons.com/wos-op/researcher/1814905/oksana-v-bondar-pidhurska/*

***Scopus Author ID:*** *https://www.scopus.com/results/authorNamesList.uri?sort=count-*

***Хоменко Ірина Іванівна*** *– старший науковий співробітник, Центр досліджень інтелектуальної власності та трансферу технологій НАН України (вул. Володимирська, 54, Київ, 01601, Україна)*

***E-mail:*** *khomenko@nas.gov.ua*

***ORCID:*** *http://orcid.org/0000-0002-8600-3848*

*UDC 330.341.1: 316.42*
*JEL Classification: L86*

***Bondar-Pidhurska O. V., Khomenko I. I. Scientific and Methodological Principles of Assessing the Efficiency of the Information Security Process Management of Small and Medium-Sized Businesses: Cybersecurity and Intellectual Property***

*The aim of the article is to study the scientific and methodological foundations of assessing the efficiency of the information security management process of small and medium-sized businesses and develop recommendations for improving its efficiency in the face of growing challenges and threats to cybersecurity and intellectual property. The main research methods were: analysis, synthesis, generalization, tabular, graphical, and integrated approach. The importance and necessity of timely assessment of the efficiency of the information security management process of small and medium-sized businesses due to the growing cyberthreats to their intellectual property as a basis for innovative development in a pandemic, war, digitalization was highlighted. The process of information security management for the protection of intellectual property (IPR) was substantiated as a reliable basis for innovative development of small and medium-sized businesses. Emphasis is placed on the growing importance, role and importance of cybersecurity for the functioning and development of small and medium-sized businesses in the face of new challenges and threats. A scientific and methodological approach to assessing the efficiency of the information security management*

*process in the context of IPR protection of small and medium-sized enterprises in the conditions of a growing number of challenges and threats has been developed and proposed for use. Emphasis was placed on the expediency of a detailed study of directions for improving the regulatory framework for information security to protect the IPR of small and medium-sized businesses in the face of countering the cyber threats. Prospective directions of research on this issue were highlighted: development of information security strategy for IPR protection in the context of prevention of new challenges and threats; improving the organizational aspects of information security management for the protection of IPR; development of digital culture of small and medium-sized businesses as a factor in improving the efficiency of the information security management process in the face of digitalization challenges.*

***Keywords:*** *information security, small and medium-sized businesses, cybersecurity, intellectual property, efficiency assessment, management process.*

***Fig.:*** *4.* ***Tabl.:*** *1.* ***Bibl.:*** *15.*

***Bondar-Pidhurska Oksana V.*** *– Doctor of Sciences (Economics), Associate Professor, Associate Professor of the Department of Management, Poltava University of Economics and Trade (3 Kovalia Str., Poltava, 36014, Ukraine)*

***E-mail:*** *Bondarpodgurskaa@gmail.com*

***ORCID:*** *http://orcid.org/0000-0001-7792-4023*

***Researcher ID:*** *https://publons.com/wos-op/researcher/1814905/oksana-v-bondar-pidhurska/*

***Scopus Author ID:*** *https://www.scopus.com/results/authorNamesList.uri?sort=count-*

*Khomenko Iryna I. – Senior Research Fellow, Intellectual Property and Technology Transfer Center of Ukraine NAS (54 Volodymyrska Str., Kyiv, 01601, Ukraine)*

***E-mail:*** *khomenko@nas.gov.ua*

***ORCID:*** *http://orcid.org/0000-0002-8600-3848*

**Вступ.** Український Уряд визначив розвиток підприємств малого та середнього бізнесу (МСП) своїм пріоритетом, який втілився у Стратегію МСП. З метою її реалізації КМУ затвердив План заходів, який має супроводжуватися численними національними та міжнародними ініціативами, започаткованими в останні роки задля поліпшення умов навколо МСП в Україні. При цьому ситуація навколо захисту інтелектуальної власності, патентування та інноваційної інфраструктури є вкрай обтяжливою для МСП і незалежних стартапів, які не можуть дозволити собі значні витрати на правовий супровід і не мають ефективних налагоджених бізнес-процесів, які пов'язані з правовим захистом активів компанії [1, с. 22, 56]. Це гальмує повноцінну реалізацію Стратегії МСП.

Водночас транснаціональні корпорації відводять вагому роль інтелектуальній власності у стратегіях посилення своїх позицій на світових ринках задля отримання конкурентних переваг і монополізації галузевих товарних ринків і послуг. Застосування високоефективних стратегій ведення «патентних війн», пов'язаних із переходом від захисту окремих виробів до агресивних форм захисту перспективних секторів ринку наукомісткої продукції та формуванням потужного портфеля патентів для блокування науково-технічних розробок і виробництва конкуруючих компаній, змінило умови реалізації прав інтелектуальної власності [2].

Водночас стрімке збільшення обороту різноманітної інформації (включаючи комерційну інформацію, інформацію про нові технології, інформацію у складі баз даних і решта), глобалізація доступу до неї та поява нових засобів її формування, поширення та використання актуалізували питання безпеки та легального застосування масивів інформації.

Інформаційна та кібербезпеки вийшли за рамки потреб окремих власників і стали одним із напрямів національних стратегій розвитку та обов'язковою субсферою діяльності підприємств як великого, так і малого та середнього бізнесу [3].

Інформаційна безпека нині стає середовищем функціонування інноваційної економіки сталого розвитку, а інформація – першопричиною явищ і процесів. При цьому національне господарство стає відкритою економічною системою глобального характеру, сталий розвиток якого забезпечується завдяки обміну із зовнішнім середовищем відповідно до змістовного ланцюга *«інформація – знання (енергія) – інновація (матерія) – задоволення ЖВІ населення країни».* Кожна його складова відповідає певному типу економіки (інформаційній – Ф. Хайєка й Е. Тоффлера, знанієвій – Д. Белла, інноваційній – П. Друкера), спричиняючи взаємодифузію [4].

Стрімке збільшення обороту різноманітної інформації (включаючи комерційну інформацію, інформацію про нові технології, інформацію у складі баз даних), глобалізація доступу до неї та поява нових засобів її формування, поширення та використання актуалізували питання безпеки та легального використання масивів інформації. А зростання ролі кібербезпеки підіймає на новий рівень питання важливості ефективного управління інформаційною безпекою підприємств малого та середнього бізнесу та захисту інтелектуальної власності.

Отже, в умовах посилення конкуренції, цифровізації економіки, пандемії Covid-19, зростання все нових викликів і загроз задоволенню життєво важливим інтересам (ЖВІ) населення України, а також функціонуванню та розвитку підприємств малого та середнього бізнесу, збереженню та примноженню їх інтелектуальної власності питання управління їх інформаційною та кібербезпекою потребують підвищеної уваги та набувають особливої актуальності, бо наслідки кіберзагроз і незаконних дій в інформаційно-комунікаційному середовищі призводять не лише до майнових, а й до репутаційних втрат для власників інформації.

**Метою** статті є дослідження науково-методичних засад оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу та розробка рекомендацій щодо підвищення його ефек-

тивності в умовах зростання кіберзагроз їх інтелектуальній власності.

**Виклад основного матеріалу.** Питання інформаційної та кібербезпеки досліджували вітчизняні та зарубіжні автори – В. Бурячок [5], О. Бондар-Підгурська [6], А. Гребенюк [7], А. Карцхия [5], Л. Рибальченко [7], В. Толубко [5], С. Толюпа[5], В. Хорошко [5], І. Хоменко [6]. Інтелектуальну власність і винахідництво як основу інноваційного розвитку підприємств висвітлено в працях Н. Аралова [8], О. Бондар [10], Ю. Капіци [8], А. Карцхия [5], Т. Косско [8], Т. Маланчук [9], Д. Махновського [8], В. Мухопада [3], І. Хоменко [8], М. Туро [8]. Проте питання оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу з позиції протистояння кіберзагрозам її інтелектуальній власності потребують висвітлення та більш детального дослідження на основі комплексного підходу.

Структурно-логічну схему дослідження на тему «Науково-методичні засади оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу: кіберзагрози та інтелектуальна власність» у загальному вигляді наведено на рис. 1.

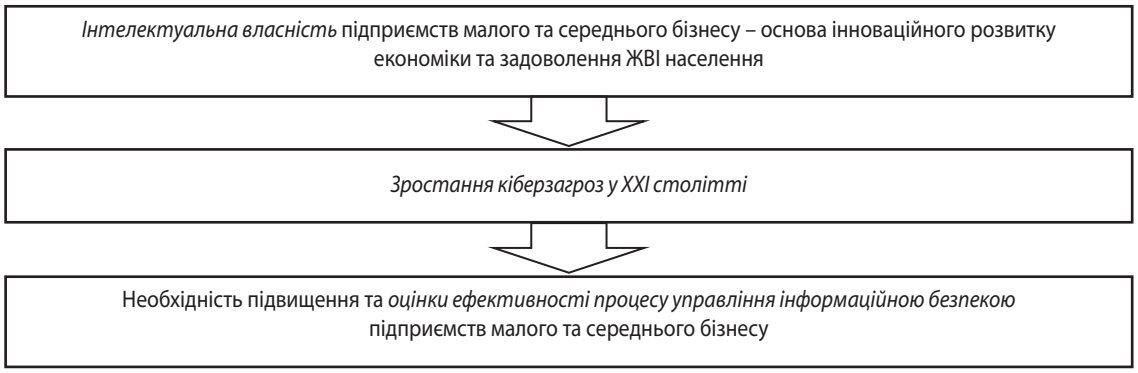


**Рис. 1. Структурно-логічна схема дослідження**

*Джерело:* авторська розробка

Інтелектуальна власність використовується в усіх видах економічної діяльності, її варто розглядати як знання, що мають цінність нині та в майбутньому, а також актив, здатний створювати реальну вартість. Стати успішним у бізнесі можливо лише шляхом розробки результативної стратегії та застосування методик управління, котрі дозволяють здійснювати ідентифікацію, надбання прав, правову охорону та ефективне використання об'єктів права інтелектуальної власності, створених або придбаних їх підприємствами [8].

Використання інтелектуальної власності в статутному капіталі підприємств, в тому числі малого і середнього бізнесу дозволяє: «1) сформувати значний за своїми розмірами статутний капітал без відволікання коштів і забезпечити доступ до банківських кредитів та інвестицій, використовуючи інтелектуальну власність як об'єкт застави нарівні з іншими видами майна; 2) амортизувати інтелектуальну власність у статутному капіталі й замінити її реальними коштами, включно з амортизаційними відрахуваннями на собівартість продукції, тобто капіталізувати інтелектуальну власність; 3) авторам і підприємствам-власникам інтелектуальної власності – стати засновниками (власниками) під час організації дочірніх і самостійних підприємств без відгалуження коштів. Водночас внесення прав на ОІВ до статутного капіталу замість «живих грошей» надає право на: 1) отримання частки прибутку (дивідендів); 2) участь в управлінні підприємством через загальні збори акціонерів; 3) отримання ліквідаційної квоти в разі ліквідації підприємства тощо» [9, с. 63].

Результатами інтелектуальної власності (ІВ) є винаходи, корисні моделі, знаки для товарів і послуг, промислові зразки, комп'ютерні програми, ноу-хау, конфіденційна інформація, котра належать до основних нематеріальних активів будь-якої організації чи підприємства, зокрема МСП. Ці активи можна використовувати, продавати, надавати право користування, а також створювати політику та імідж підприємства.

При цьому здійснення винахідницької діяльності безпосередньо пов'язане з наявністю або відсутністю в країні сприятливих умов для генерування ІВ та їх використання, що визначені ВОІВ:

1) забезпечення високого рівня фінансування наукових досліджень;
2) наявність системи підтримки інновацій;
3) наявність засобів державної підтримки (фінансової, податкової, організаційної, спрямованої на збільшення генерації винаходів та інших ОІВ науковими установами, вільними економічними зонами, підприємствами, у тому числі малими підприємствами);
4) наявність коштів для державної підтримки комерціалізації ІВ, передачі технологій науковими організаціями;
5) наявність ефективної інфраструктури для комерціалізації ІВ і передачі технологій;
6)доступність освіти у сфері ІВ тощо [11].

Зауважимо, що у 1994-2018 рр. характерною особливістю України була практична відсутність будь-яких важелів інновацій, трансферу технологій, комерціалізації ОІВ у країні, а також відсутність стратегічних документів, що визначають інноваційний розвиток і розвиток ІВ. Це суттєво відрізняло Україну від країн-членів ЄС, а також таких

держав, як Білорусь, Казахстан та інші. Проте, у 2019 році відбулися певні позитивні зміни. Так, за спільною ініціативою ВОІВ і Мінекономрозвитку України було підготовлено Національним відомством ІВ за участю групи експертів проєкт Національної стратегії розвитку інтелектуальної власності в Україні на 2020–2025 роки. Проєкт став комплексним документом, який надає аналіз стану державного управління, законодавства, формування та використання прав ІВ і заходів державної підтримки цієї діяльності. Проєкт «Побудова ефективної системи захисту інтелектуальної власності в Україні» обговорювався під час парламентських слухань 16 грудня 2019 року. З часом Кабінет Міністрів України затвердив Стратегію розвитку інноваційної діяльності на період до 2030 року (наказ від 10.07.2019 № 526-р) [8]. Водночас питання щодо захисту ОІВ від кіберзагроз у «Стратегії кібербезпеки України» від 14 травня 2021 року не знайшло належного відображення [12].

Значення захисту цінних технологій, ОІВ та інформації від крадіжки, шпигунства або інших методів незаконного присвоєння зростає через чинники глобалізації, подовження ланцюжка постачання товарів, широкого використання інформаційно-комунікаційних технологій, використання аутсорсингу тощо. Збільшуються ризики того, що вкрадена комерційна інформація (trade secrets) буде використовуватись у країнах-конкурентах. Серйозне занепокоєння викликають загрози бізнесу від промислового та економічного шпигунства. Особливого значення набуває безпека та захист комерційної інформації (комерційних секретів), якими володіють працівники під час виконання своїх функціональних обов'язків [3, с. 50]. Протягом останніх 2 років кількість інцидентів щодня зростає. До цього переліку нині додаються кіберзагрози. Число кібератак у світі зросло в 40 разів: 1 млн «нальотів» припадає на Україну щотижня. За кількістю кібератак Україна знаходиться на 17-му місці у світі, 50 % усіх кібератак припадає на підприємства малого та середнього бізнесу [13].

Кібербезпека стала головним пріоритетом для організацій нині: 85 % респондентів в усьому світі заявили, що вона надзвичайно важлива або важливіша, ніж була до пандемії [14, с. 8]. А в період воєнного часу ця значущість зростає. Частку підприємств малого, середнього і великого бізнесу, співробітники яких (більша половина) працюють віддалено, наведено на рис. 2.

При цьому діаграма глобального відсотку важливості кібербезпеки свідчить, що 85 % респондентів визнають її переважаючу роль (рис. 3).

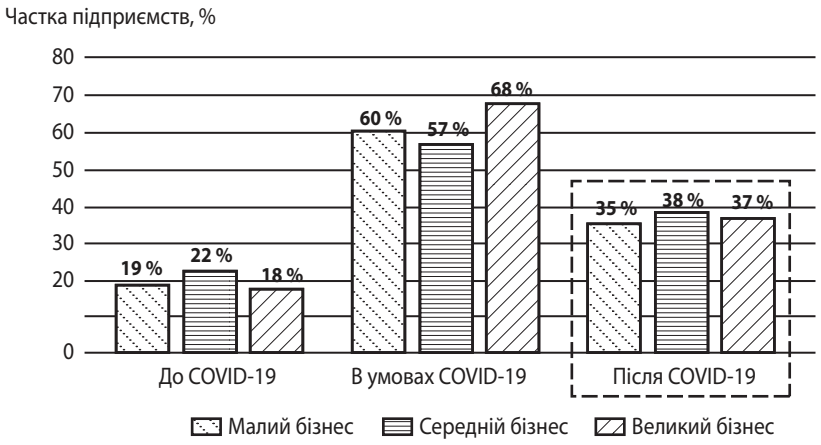


**Рис. 2. Частка підприємств, співробітники яких (більша половина) працюють віддалено: малий, середній і великий бізнес**

*Джерело:* адаптовано авторами на основі опрацювання джерела [14, с. 7]

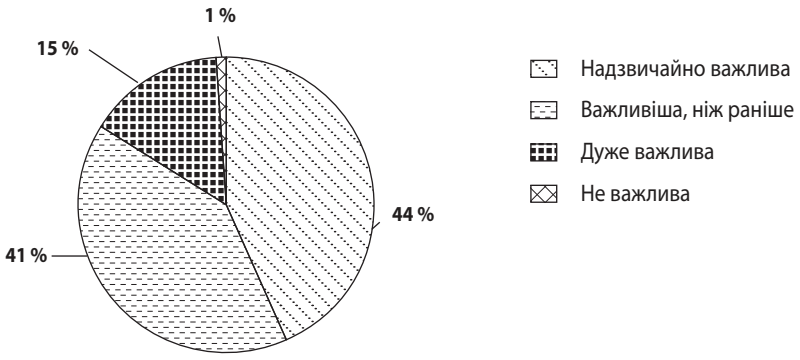


**Рис. 3. Глобальний відсоток важливості кібербезпеки**

*Джерело:* адаптовано авторами на основі опрацювання джерела [14, с. 7]

Розглядаючи детальніше, значна частина респондентів Азійсько-Тихоокеанський регіону (44 %) і Америки (50 %) заявили, що кібербезпека *надзвичайно важлива* для їхнього бізнесу. З іншого боку, в Європі було більше респондентів, які вказали, що вона важливіша, ніж була раніше, на 46 %. При чому така тенденція також є характерною для малого, середнього і великого бізнесу: 79 %, 87 % і 88 % відповідно.

До того ж реальні прояви кібератак важко прогнозовані, а їх результатом стають значні фінансово-економічні збитки або непередбачувані наслідки у порушенні функціонування інформаційно-телекомунікаційних систем, які впливають на стан фінансової й економічної безпеки бізнесу. Прикладом такої кібератаки, котру не можна було спрогнозувати, є виведення з ладу понад 70 урядових сайтів у ніч з 13 на 14 січня 2022 року через хакерські атаки. Внаслідок цього менеджмент бізнесу був позбавлений можливості зайти на будь-який сайт міністерства та дізнатися про потрібну йому інформацію.

До найпоширеніших кібератак для підприємств малого та середнього бізнесу слід віднести фішинг (атака, яка переважно використовує електронну пошту і обманом змушує людей завантажувати шкідливі програми на пристрої), а також витік даних (відбувається, коли конфіденційна інформація користувача стає вразливою). Так, кіберпростір стає середовищем, де існує велика кількість суб'єктів, метою діяльності яких є заволодіння особистими даними споживачів, даними бізнес-суб'єктів платіжними системами, коштами чи особистими даними інтернет-користувачів [15].

При цьому найрозповсюдженіші проблеми, які зустрічаються у малому та середньому бізнесі, такі:

1) незахищеність периметра (неналаштований мережевий захист, неналаштований захист серверів і кінцевих пристроїв, відсутність систем моніторингу та системи резервного копіювання з часом призводить до пошкодження ІТ-інфраструктури);
2) незахищеність інформації та баз даних (бухгалтерська та фінансова інформація, звіти до контролюючих органів, база даних клієнтів, листування з важливими клієнтами або партнерами, особиста конфіденційна інформація тощо);
3) незахищеність каналів передачі (більшість компаній сьогодні потребують доступу до своєї ІТ-інфраструктури 24/7 із будь-якої точки світу. Для ефективної роботи їм необхідний швидкий, безпечний канал передачі інформації. Це розуміють керівники, а також зловмисники, тому часто замість атаки на ІТ-інфраструктуру вибирають атаку на канали передачі інформації);
4) неналежний антивірусний захист (щодня з'являються нові комп'ютерні віруси, котрі виконують завдання від збирання інформації до шифрування інформації чи використання шкідливих дій);
5) неналежний захист сайту (якщо вас немає в Інтернеті, вас немає у бізнесі);
6) неналежний захист програм і додатків (пошта, месенджери, програми, які використовують для роботи та спілкування з клієнтами).

До втрати репутації, коштів, а іноді й клієнтів можуть призвести пошкодження програм і каналів спілкування, викрадення конфіденційних даних і розсилка через них шкідливої інформації. В результаті вищезгаданих загроз є ризик втрати надважливих даних (sensitive data) [13]. Відповідно, процес управління інформаційною безпекою щодо захисту ОІВ (нематеріальних активів) на підприємствах МСБ необхідно ретельно продумувати, розробляти та втілювати. Наприклад, зберігати важливу інформацію з режимом охорони як ноу-хау або як комерційну таємницю, або запатентувати її як винахід чи як корисну модель, зареєструвати знак для товарів і послуг тощо.

Крім того, варто ідентифікувати ризики та загрози, а також започаткувати кіберзахист ОІВ підприємств малого та середнього бізнесу, що починається, як правило, з аудиту інформаційних потоків, аудиту баз і середовища зберігання, права доступу до інформації, кіберзагроз, мережі, серверів, програм, сервісів, додатків і робочих місць кінцевих користувачів. Наступним етапом є розвиток, підтримка та обслуговування реалізованих рішень, що пов'язано з навчанням персоналу, його участю в американських та європейських програмах, послугами аутсорсингу з кібербезпеки тощо [15].

Отже, інформація нині стає надзвичайно важливим ресурсом, який цікавий для комп'ютерних злодіїв. З метою упередження кібератак топ-менеджменту МСП варто вчасно попіклуватися про їх кібербезпеку. Вищевикладене стало підставою для візуалізації архітектоніки процесу управління інформаційною безпекою підприємств малого та середнього бізнесу щодо захисту ОІВ в умовах нових викликів і загроз (рис. 4).

Завдання підвищення ефективності захисту інтелектуальної власності від нових кібезагроз пов'язані з розширенням різноманітності самих об'єктів інтелектуальної власності. Проблеми захисту доменних імен різного рівня та товарних знаків, глобалізація інтернет-торгівлі та інших послуг у мережі Інтернет (включаючи електронну біржу інтелектуальної власності), розповсюдження «віртуальних» грошей та інтернет-валют, розширення можливостей 3D-принтінгу, суттєвого підвищення вимог до кібербезпеки персональних даних та інформаційних баз даних, захист авторських прав і прав особи в інтернеті (включаючи право авторства, право на «особистий імідж» або «особисті бренди») [3, с. 49].

Нові виклики потребують нового науково-методичного забезпечення, вчасних адекватних оцінок і відповідей, результативних рішень, а також обумовлюють необхідність підвищення ефективності процесу управління інформаційною безпекою підприємств щодо захисту ОІВ від кіберзагроз.

Викладене дозволило сформувати науково-методич_ний підхід щодо оцінки ефективності процесу управління інформаційною безпекою в контексті захисту ОІВ підприємств МСБ в умовах загроз їх кібербезпеці (табл. 1).

**Висновки**. Таким чином, актуалізовано питання управління інформаційною безпекою щодо захисту об'єктів інтелектуальної власності підприємств малого і середнього бізнесу в контексті протистояння кіберзагрозам, чисельність яких щоденно зростає. Наголошено на необхідності розроб-

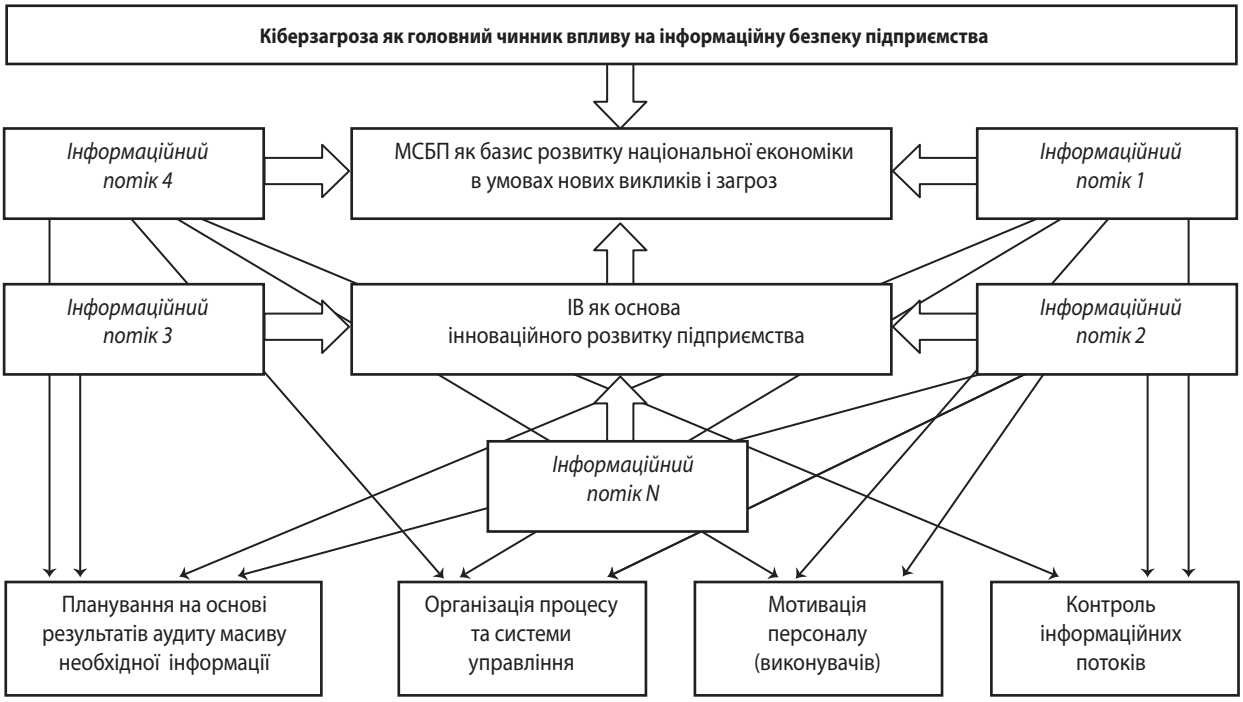


**Рис. 4. Архітектоніка процесу управління інформаційною безпекою щодо захисту ОІВ підприємств малого та середнього бізнесу в умовах нових викликів і загроз**

*Джерело:* авторська розробка

**Таблиця 1**

**Візуалізація науково-методичного підходу щодо оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу в контексті захисту їх ОІВ (Y)**

| Індикатори, показники, напрями аналізу | Зміст індикатору розвитку закладу | Фактичний стан | Відхилення | Перспективні напрями усунення недоліків |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| *Загальні маркери оцінки (X1)* | | | | |
| Планування (X1.1) | Наявність розробленої концепції та чіткої стратегії розвитку інформаційної безпеки щодо захисту ОІВ підприємств МСБ, врахування результатів аудиту | … | … | … |
| Організація (X1.2) | Наявність відділу (сектора, відповідального, CISO) інформаційної безпеки щодо захисту ОІВ підприємств МСБ | … | … | … |
| Мотивація (X1.3) | Заохочення якісного виконання функціональних обов'язків щодо інформаційної безпеки щодо захисту ОІВ підприємств МСБ | … | … | … |
| Контроль (X1.4) | Наявність всіх видів контролю на підприємствах щодо здійснення процесу управління інформаційною безпекою ОІВ МСБ | … | … | … |
| Координація (X1.5) | Синхронне виконання вищезазначених функцій процесу управління інформаційною безпекою щодо захисту ОІВ МСБ | … | … | … |
| *Спеціальні маркери оцінки (X2)* | | | | |
| Методи запобігання інформаційним загрозам (X2.1) | 1) резервне копіювання; | … | … | … |

**Закінчення табл. 1**

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| | 2) політика прав доступу (обмеження кола людей, які мають права доступу до важливих даних підприємства;<br>3) двофакторна аутентифікація | | | |
| Механізми запобігання інформаційним загрозам (X2.2) | Фізичний, особистий і організаційний | … | … | … |
| Рівень інформованості та ступінь використання основних (функціональних) критеріїв інформаційної безпеки (конфіденційність, цілісність, доступність) (X2.3) | Наявність і використання моделі тріади CIA (англ. Confidentiality, Integrity and Availability) або конфіденційність, цілісність, доступність | … | … | … |
| Рівень дотримання критерію гарантій (X2.4) | Дозволяє оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації | … | … | … |
| Рівень дотримання критерію додаткових властивостей інформаційної безпеки щодо захисту ОІВ підприємств МСБ в умовах нових викликів і загроз (X2.5) | До них відносять:<br>1) апелювання (англ. non-repudiation) – можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший;<br>2) підзвітність (англ. accountability) – властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об'єктів та однозначно встановлювати авторів певних дій в системі;<br>3) вірогідність (англ. reliability) – властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце;<br>4) автентичність (англ. authenticit) – властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим | … | … | … |
| Наявність сертифікації ISO 27001 | ISO 27001 – це міжнародний стандарт, який встановлює вимоги до створення, впровадження, моніторингу, обслуговування та вдосконалення системи менеджменту інформаційної безпеки від спроб несанкціонованого доступу. Нині корпоративна інформаційна безпека для МСП – це не лише комплекс технічних засобів, таких як антивіруси, а підхід до поводження з активами підприємства загалом | … | … | … |
| Висновки…<br>Y = F(X1; X2) | | | | |

*Джерело:* авторська розробка

ки науково-методичного забезпечення щодо вчасної оцінки ефективності цього процесу менеджментом підприємств.

З цією метою узагальнено критерії оцінки інформаційної безпеки в контексті захисту ОІВ підприємств малого і середнього бізнесу: функціональні (тріада CIA), додаткові та гарантійні критерії. Виокремлено рівні інформаційної безпеки (у тому числі державний; підприємства (у т. ч. ОІВ); захист інформаційної безпеки особистості), а також функції, методи, механізми захисту та запобігання загрозам (а саме: фізичний, особистий та організаційний), наявність системи сертифікації ISO 27001. На підставі викладеного розроблено та запропоновано до використання науково-методичний підхід до оцінки ефективності процесу управління інформаційною безпекою щодо захисту ОІВ підприємств малого і середнього бізнесу в умовах протистояння кіберзагрозам, що повинно сприяти підвищенню результативності його управління загалом, зростання рівня їх конкурентоспроможності та стійкості.

Рекомендовано перспективні напрями досліджень цієї проблематики: розробка стратегії інформаційної безпеки щодо захисту ОІВ у контексті попередження нових викликів і загроз; удосконалення організаційних аспектів управління інформаційною безпекою щодо захисту ОІВ; розвиток цифрової культури підприємств малого і середнього бізнесу як чинника підвищення ефективності процесу управління інформаційною безпекою в умовах викликів діджиталізації. Крім того, є сенс розглянути напрями удосконалення нормативно-законодавчої бази з питань управління інформаційною безпекою щодо захисту ОІВ підприємств малого і середнього бізнесу в умовах протистояння кіберзагрозам.

**ЛІТЕРАТУРА**


**1.** Великі проблеми малого бізнесу: оцінка реалізації стратегії розвитку малого та середнього підприємництва в Україні на період до 2020 року та подальші напрями політики: системний звіт. Київ : БЦ «Поділ Плаза», 2021. URL: https://boi.org.ua/media/uploads/system_bigproblemssmalbusiness/3_2020_system_ua.pdf

**2.** Мухопад В. И. Коммерциализация интеллектуальной собственности. М. : Магистр, 2010. 512 с.

**3.** Карцхия А. А. Кибербезопасность и интеллектуальная собственность. *Вопросы кибербезопасности* 2014. № 1 (2). С. 61–66.

**4.** Бондар-Підгурська О. В. Науково-методологічні засади сталого інноваційного соціально орієнтованого розвитку економіки. Полтава : РВВ ПУЕТ, 2016. 531 с.

**5.** Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

**6.** Bondar-Pidhurska O. V., Khomenko I. I. Peculiarities of evaluation of efficiency of the process of information security management of the enterprise: cyber security and intellectual propert. *Modern scientific research: achievements, innovations and development prospects*. Proceedings of the 8th International scientific and practical conference. MDPC Publishing. Berlin, Germany. 2022. P. 632–638.

**7.** Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.

**8.** Капіца Ю. М., Косско Т. Г. Махновський Д. С., Хоменко І. І., Аралова Н. І., Туров М. П. Винахідницька діяльність у наукових установах. Київ : Логос, 2021. 455 с.

**9.** Маланчук Т. В. Бізнес-право та інтелектуальна власність : конспект лекцій. Суми : СумДУ, 2019. 77 с.

**10.** Бондар О. В. Особливості та проблеми управління комерціалізацією технологій як умови сталого інноваційного розвитку та конкурентоспроможності України // Актуальні питання розвитку економіки: теорія і практика : кол. моногр. / за ред. А. О. Касич, М. М. Хоменко. Кременчук : Кременчуцька міська друкарня, 2012. С. 8–15.

**11.** Methodology for the Development of National Intellectual Property Strategies. Tool 1 : The Process, WIPO, 2016. URL: https://www.wipo.int/ipstrategies/en/methodology/

**12.** Указ Президента України №447/2021. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL: https://www.president.gov.ua/documents/4472021-40013

**13.** Нестеренко Михаил. Кибербезопасность малого и среднего бизнеса: топ-6 угроз и проблем, которые нужно решать уже сейчас. 2022. 09 января // UBR 2007–2022. URL: ubr.ua/blog/praktika-biznesa/kiberbezopasnost-maloho-i-srednehobiznesa-top-6-uhroz-i-problem-kotorye-nuzhno-reshat-uzhesejchas-4011165

**14.** Звіт про перспективи безпечної віддаленої роботи. Cisco SecureX™. 2021. URL: https://www.cisco.com/c/dam/global/uk_ua/products/future-of-secure-remote-work-report.pdf

**15.** Бутина Мария. Кибербезопасность предприятия: что учесть? *Безопасность бизнеса*. 2022. 16 февраля // Інформаційне агентство «Ліга:Закон». URL: https://jurliga.ligazakon.net/ru/news/209245_kiberbezopasnost-predpriyatiya-chto-uchest


**REFERENCES**


Bondar, O. V. "Osoblyvosti ta problemy upravlinnia komertsializatsiieiu tekhnolohii yak umovy staloho innovatsiinoho rozvytku ta konkurentospromozhnosti Ukrainy" [Peculiarities and Problems of Managing Technology Commercialization as a Condition for Sustainable Innovative Development and Competitiveness of Ukraine]. In *Aktualni pytannia rozvytku ekonomiky: teoriia i praktyka*, 8-15. Kremenchuk: Kremenchutska miska drukarnia, 2012.

Bondar-Pidhurska, O. V. *Naukovo-metodolohichni zasady staloho innovatsiinoho sotsialno oriientovanoho rozvytku ekonomiky* [Scientific and Methodological Foundations of Sustainable Innovative Socially Oriented Development of the Economy]. Poltava: RVV PUET, 2016.

Bondar-Pidhurska, O. V., and Khomenko, I. I. "Peculiarities of evaluation of efficiency of the process of information security management of the enterprise: cyber security and intellectual propert". *Modern scientific research: achievements, innovations and development prospects*. Berlin, Germany: MDPC Publishing, 2022. 632-638.

Butina, M. "Kiberbezopasnost predpriyatiya: chto uchest? Bezopasnost biznesa. 2022. 16 fevralya" [Enterprise Cybersecurity: What to Consider? Business Security. February 16, 2022]. Informatsiine ahentstvo «Liha:Zakon». https://jurliga.ligazakon.net/ru/news/209245_kiberbezopasnost-predpriyatiya-chto-uchest

Hrebeniuk, A. M., and Rybalchenko, L. V. *Osnovy upravlinnia informatsiinoiu bezpekoiu* [Fundamentals of Information Security Management]. Dnipro: Dniprop. derzh. un-t vnutrish. sprav, 2020.

*Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* [Information and Cyber Security: Socio-technical Aspect]. Kyiv: DUT, 2015.

Kapitsa, Yu. M. et al. *Vynakhidnytska diialnist u naukovykh ustanovakh* [Inventive Activity in Scientific Institutions]. Kyiv: Lohos, 2021.

Kartskhiya, A. A. "Kiberbezopasnost i intellektualnaya sobstvennost" [Cyber Security and Intellectual Property]. *Voprosy kiberbezopasnosti*, no. 1(2) (2014): 61-66.

[Legal Act of Ukraine] (2021). https://www.president.gov.ua/documents/4472021-40013

"Methodology for the Development of National Intellectual Property Strategies. Tool 1 : The Process". WIPO, 2016. https://www.wipo.int/ipstrategies/en/methodology/

Malanchuk, T. V. *Biznes-pravo ta intelektualna vlasnist : konspekt lektsii* [Business Law and Intellectual Property: Lecture Notes]. Sumy: SumDU, 2019.

Mukhopad, V. I. *Kommertsializatsiya intellektualnoy sobstvennosti* [Commercialization of Intellectual Property]. Moscow: Magistr, 2010.

Nesterenko, M. "Kiberbezopasnost malogo i srednego biznesa: top-6 ugroz i problem, kotoryye nuzhno reshat uzhe seychas. 2022. 09 yanvarya" [Cybersecurity for Small and Medium Businesses: top 6 Threats and Problems That Need to Be Addressed Now. January 09, 2022]. UBR 2007-2022. ubr.ua/blog/praktika-biznesa/kiberbezopasnost-maloho-i-sredneho-biznesa-top-6-uhroz-i-problem-kotorye-nuzhno-reshat-uzhe-sejchas-4011165

"Velyki problemy maloho biznesu: otsinka realizatsii stratehii rozvytku maloho ta serednyoho pidpryiemnytstva v Ukraini na period do 2020 roku ta podalshi napriamy polityky: systemnyi zvit" [Major Problems of Small Business: Evaluation of the Implementation of the Strategy for the Development of Small and Medium-sized Enterprises in Ukraine for the Period until 2020 and Further Directions of the Policy: A Systematic Report]. Kyiv : BTs «Podil Plaza», 2021. https://boi.org.ua/media/uploads/system_bigproblemssmalbusiness/3_2020_system_ua.pdf

"Zvit pro perspektyvy bezpechnoi viddalenoi roboty. Cisco SecureX™" [A Report on the Outlook for Secure Remote Work. Cisco SecureX™]. 2021. https://www.cisco.com/c/dam/global/uk_ua/products/future-of-secure-remote-work-report.pdf

Стаття надійшла до редакції 03.05.2022 р.