МАКОВЕЦЬ
Оксана Петрівна
banzhulka@ukr.net

УДК 336.63

ДРОЗД
Ірина Кузьмівна

КІБЕРБЕЗПЕКА ЯК ФАКТОР ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

CYBERSECURITY AS FACTOR OF FINANCIAL SECURITY OF THE ENTERPRISE

DOI: https://doi.org/10.37634/efp.2020.5(3).8

студентка, Київський національний університет імені Тараса Шевченка, Інститут післядипломної освіти

д.е.н., професор, Київський національний університет імені Тараса Шевченка, Інститут післядипломної освіти

MAKOVETS Oksana Petrivna *– student, Institute of Postgraduate Education of Kyiv National University after Taras Shevchenko*

DROZD Iryna Kuzmivna *– Doctor of Economics, Professor, Institute of Postgraduate Education of Kyiv National University after Taras Shevchenko*

У статті розглядається необхідність забезпечення належного рівня фінансової безпеки підприємства скрізь призму існування такого виду втручання у діяльність суб'єктів господарювання як кіберзагрози. Для всебічного та об'єктивного висвітлення проводиться огляд таких теоретичних понять як фінансова безпека підприємства, кіберзагроза, кібербезпека, кіберзахист у їх взаємозв'язку. Проводиться огляд досліджень у сфері кібербезпеки. Основна увага зосереджена на висвітленні збитків та втрат для бізнесу, які за собою тягнуть кібератаки. Авторами запропоновано враховувати категорії кіберзагроза та кібербезпека у дослідженні питання інвестиційної привабливості підприємства.

* * *

В статье рассматривается необходимость обеспечения надлежащего уровня финансовой безопасности предприятия сквозь призму существования такого вида вмешательства в деятельность субъектов хозяйствования как киберугрозы. Для всестороннего и объективного освещения проводится обзор таких теоретических понятий как финансовая безопасность предприятия, киберугрозы, кибербезопасность, киберзащита в их взаимосвязи. Проводится обзор исследований в области кибербезопасности. Основное внимание сосредоточено на освещении убытков и потерь для бизнеса, которіе возникают вследствии кибератак. Авторами предложено учитывать категории киберугроз и кибербезопасность при исследовании вопроса инвестиционной привлекательности предприятия.

* * *

Introduction. *As a component of the business environment the information environment is characterized by significant cyber threats and requires cyber protection. The processes of Ukrainian society digitalization and changes in providing the information security update the enterprise's financial security measures and their connection with cybersecurity.*

The purpose of the paper *is to analyze the essence of cybersecurity as a factor of the enterprise's financial security and to identify its impact on the investment attractiveness of the business entity. To achieve the purpose the task is to explore the concepts of financial security, cybersecurity and cyber threats, to identify their relationship and impact on business' financial losses of the, the consequences for the enterprise's investment attractiveness. The study will provide information on business management and plan effective policies to combat cyber threats.*

Results. *The essence of enterprise's financial security is investigated. There are three approaches in identifying the essence of this concept, including as part of the enterprise's economic security, as the state of the most effective use of information, financial indicators and as its financial condition level, which provides stable protection of priority balanced financial interests from real and potential external and internal threats. These definitions are used to substantiate the connection with the concepts of cyber threat and cyber security. The areas of possible losses based on the losses assessment due to cyber threats are identified by the authors, namely the intellectual property loss, the business information loss, the IT systems' continuity disruption, the reputation damage as a result of the attack, the automated personal data loss.*

Conclusion. *It is concluded that the necessary measures of cybersecurity, protection of enterprises' information resources and prevention of unauthorized interference in the enterprises' activities, which has a positive effect on investment attractiveness and increases the enterprises' competitiveness.*

Ключові слова: *фінансова безпека, кіберзагрози, інформаційна безпека, кібербезпека, втрати підприємства, інвестиційна привабливість*

Ключевые слова: *финансовая безопасность, киберугрозы, информационная безопасность, кибербезопасность, потери предприятия, инвестиционная привлекательность*

Keywords: *financial security, cyber threats, informational security, cybersecurity, losses of the enterprise, investment attractiveness*

ВСТУП

У сучасних умовах цифровізації українського суспільства та змін до підходів забезпечення захисту інформації стає актуальним питання фінансової безпеки підприємства та її зв'язку з кібербезпекою. Ще декілька років тому кібербезпека як елемент захисту від кіберзагроз підприємства не мала належного врегулювання на законодавчому рівні. Лише після масштабних кібератак на державні установи, у т.ч. на фінансові органи управління України, було розпочато роботу за даним напрямком. У динамічному економічному середовищі вітчизняні підприємства стикаються з новими інформаційними внутрішніми та зовнішніми загрозами, які негативно впливають як на їх фінансову стабільність, так і на інвестиційну привабливість. Слід відмітити, що значне місце серед зовнішніх загроз впливу на фінансову безпеку підприємства посідає таке достатньо нове поняття для українського бізнесу, як кіберзагрози.

Вивченню питання фінансової безпеки підприємства присвячені роботи науковців О.І. Судакової, Т.Б. Кузенко, І.О. Бланка, поняття кібербезпеки, кіберзагрози, кіберпростору досліджено В.М. Фурашевим, Н.М. Пантєлєєвою, Л.В. Романовською, М.С. Романовською, поняття та аспекти інвестиційної привабливості підприємств розглядали О.В. Носова, С.О. Євтушенко, Н.Ю. Брюховецька, О.В. Хасанова. Водночас площина управління кібербезпекою задля цілей фінансової стабільності розглядаються у дослідженнях практиків, зокрема бізнес-консалтингових компаній.

В умовах сьогодення потребує поглиблення вивчення питання пов'язаності понять фінансової безпеки та кібербезпеки, як частини інформаційної безпеки, а також їх вплив на інвестиційну привабливість підприємства.

МЕТА статті – проаналізувати сутність кібербезпеки як фактору фінансової безпеки підприємства та виявити її вплив на інвестиційну привабливість підприємства. Для цього поставлено наступні завдання: дослідження поняття фінансової безпеки, сутності та змісту кібербезпеки та кіберзагроз як одного із видів загроз операційній діяльності підприємства, проведення огляду фінансових втрат бізнесу від кібератак та значення для інвестиційної привабливості підприємства.

МЕТОДИ ДОСЛІДЖЕННЯ

У процесі дослідження використано загальнонаукові методи аналізу та синтезу, методи теоретичного дослідження, методи узагальнення, порівняльний метод.

РЕЗУЛЬТАТИ

У часи тотальної діджиталізації українського суспільства належний рівень інформаційної складової фінансової безпеки підприємства є основоположним чинником для залучення інвестицій та розширення бізнесових горизонтів. Для об'єктивного розуміння досліджуваної теми, слід звернутися до поширених визначень поняття фінансової безпеки підприємства як такого.

О.І. Судакова визначає, що «фінансова безпека – це важлива складова частина економічної безпеки підприємства, що базується на незалежності, ефективності й конкурентоспроможності фінансів підприємства, яка відображається через систему критеріїв і показників його стану, що характеризують збалансованість фінансів, достатню ліквідність активів і наявність необхідних грошових резервів, фінансову стабільність, ступінь захищеності фінансових інтересів на всіх рівнях фінансових відносин [1].

Т.Б. Кузенко пов'язує фінансову безпеку з досягненням значень певних показників, а саме характеризує її як «стан найбільш ефективного використання інформаційних, фінансових показників, ліквідності та платоспроможності, рентабельності капіталу, що знаходиться в межах своїх граничних значень» [2].

Науковцем І.О. Бланком фінансову безпеку охарактеризовано виходячи з основ економічної теорії та фінансової філософії, що надає ґрунтовності даному визначенню: «кількісно і якісно детермінований рівень його фінансового стану, який забезпечує стабільну захищеність його пріоритетних збалансованих фінансових інтересів від ідентифікованих реальних і потенційних загроз зовнішнього і внутрішнього характеру, параметри яких визначаються на основі його фінансової філософії і створюють необхідні передумови фінансової підтримки його сталого розвитку у поточному й перспективному періоді» [3].

Із вказаного визначення нами виокремлено декілька важливих аспектів, які корелюються із завданнями даного дослідження, а саме:

– кількісне та якісне обумовлення фінансового стану, що зі свого боку пов'язане з інвестиційною привабливістю;

– рівень або ступінь захищеності його фінансових інтересів від потенційних загроз.

Необхідно зауважити, що, як зазначалось вище, фінансова безпека є складовою частиною економічної безпеки, та, на думку авторів, кібербезпека, як частина інформаційної безпеки, є фактором, що впливає на рівень фінансової безпеки підприємства.

У теперішніх умовах розвитку інформаційних технологій потенційні загрози фінансовим інтересам виникають на різних етапах процесу діяльності підприємства. Одним із видів загроз, які можуть істотно вплинути на всі аспекти діяльності в інформаційному просторі діяльності підприємства, є кіберзагрози.

У широкому розумінні, як визначено в Законі України від 5 жовтня 2017 р. №2163-VIII «Про основні засади забезпечення кібербезпеки України» (далі – Закон), «кіберзагроза – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів» [4]. У вузькому ж розумінні кіберзагроза у фінансовій діяльності підприємства – це втручання у операційну діяльність підприємства, яке тягне за собою втрати фінансових ресурсів, і відповідно впливає на інтереси як власників, так і інвесторів. Тобто одним із проявів порушення фінансової безпеки підприємства є кіберзагрози.

Відповідно до положень Закону «кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [4].

В.М. Фурашев вважає, що «кібербезпека – це стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації» [5, с.163].

Н.М. Пантєлєєва, Л.В. Романовська та М.С. Романовська розглядають кібербезпеку ширше, як «комплексне поняття, яке поєднує у своїй сутності предметну основу кіберпростору та процесну функціональність механізму захисту, спирається на системний та інституційний підходи, принципи ефективності, надійності, оптимальності» [6, с. 133].

У практичній площині сутність кібербезпеки – це процес захисту інтересів будь-якого суб'єкта під час використання кіберпростору, який є «інтерактивним інформаційним середовищем, що функціонує за допомогою комп'ютерних систем» [7].

Зі змістом кібербезпеки України тісно пов'язаний і кіберзахист, який є «сукупністю організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [4].

Теоретично-змістовні поняття кібербезпеки як процес захисту та захищеність ув'язуються з поняттям кіберпростору (середовищем), кіберзагрозою (об'єктом) та кіберзахистом – заходами захисту, ліквідації наслідків на підприємстві.

Тобто з поняттями достатнього рівня фінансової безпеки підприємства як рівня захищеності фінансових інтересів пов'язаний і необхідний рівень кіберстійкості підприємства, який зі свого боку відображається на фінансових показниках підприємства та його цікавості для потенційних інвесторів.

Крім цього, у теперішніх умовах розвитку економіки інвестиційна привабливість сфери кібербезпеки є визначальною, оскільки в світі відбувається стрімкий розвиток інформаційних технологій. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій. Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [8].

Сфера кібербезпеки як частина інформаційної безпеки будь-якого суб'єкта господарювання, посідає визначне місце серед найбільш обговорюваних пріоритетів майбутнього розвитку підприємств. Слід відмітити, що довгий час причиною вразливості бізнесу була неусвідомленість можливих загроз.

Згідно з дослідженням «EY Global Information Security Survey 2018-19» (GISS), проведеним компанією EY (Ernst & Young) та опублікованим на офіційному сайті встановлено, що 77 % респондентів мають базовий набір інструментів із забезпечення кібербезпеки. У більшості компанії не знають, де саме зберігаються найбільш критичні інформаційні активи й не мають гарантій щодо їхньої безпеки. Згідно з дослідженням GISS, 77 % організацій планують не тільки встановити основні засоби кібербезпеки, але й налаштувати їх відповідно до можливостей та умов бізнесу. Такі компанії не тільки впроваджують базові засоби кібербезпеки, але й переосмислюють принципи та архітектуру кібербезпеки, щоб більш ефективно підтримувати діяльність бізнесу [9].

Питанням кібер-загроз також присвячено «Дослідження глобальних тенденцій інформаційної безпеки за 2018 р.: основні висновки «Посилення цифрового середовища проти кібер-загроз» компанії PwC Ukraine, яким визначено, що «побудова вертикальної стратегії управління кіберризиками та ризиками конфіденційності вкрай необхідна в рамках усього підприємства, а концепція стійкості має бути інтегрована у комерційну діяльність. Стратегія компанії в області керування ризиками має базуватись на глибокому розумінні кіберзагроз, які стоять перед нею, та чіткому розумінні того, які ключові активи потребують найвищого рівня захисту. Необхідна цілісна концепція виявлення прийнятного рівня ризику. Керівництво має стимулювати розвиток культури управління кіберризиками на всіх рівнях організації, а стійкість до кіберзагроз має розглядатись як невід'ємний компонент отримання вигоди, а не тільки як спосіб запобігання ризикам. Зокрема, досягнення більш високого рівня стійкості до ризиків є шляхом до більш високої та довгострокової економічної ефективності» [10, с. 12].

За даними компанії McAfee, що займається розробкою антивірусного програмного забезпечення, кібер-злочинці щорічно завдають світовій економіці збитків у розмірі $600 млрд. Страховий концерн Lloyd's називає трохи скромнішу цифру – $400 млрд. на рік. За даними компанії Herjavec Group, яка спеціалізується на консалтингу у сфері кібер-безпеки, зараз у світі понад 4 млрд. користувачів Інтернету, у 2022 р. їхня кількість зросте до 6 млрд., а в 2030-му р. – до 7,5 млрд. А за прогнозами Ericsson, до 2023 р. кількість підключених до глобальної мережі пристроїв досягне 30 млрд. Це майже вдвічі більше, ніж у 2017 р.[11].

Тобто зі зростанням кількості користувачів кіберпростором зростає і фактична можливість нараження на кіберзагрози як такі.

Експерти МВФ підрахували, що економічні втрати від усіх глобальних кібернападів сягають $53 млрд., у т.ч. $850 млн. від нападу вірусу "NotPetya", що уразив у липні український фінансовий і державний сектор та створив проблеми в інших країнах [12]. За останні роки найбільш відомі кібератаки у світі це: віруси-вимагачі WannaCry та NotPetya, наведені на рис.1.

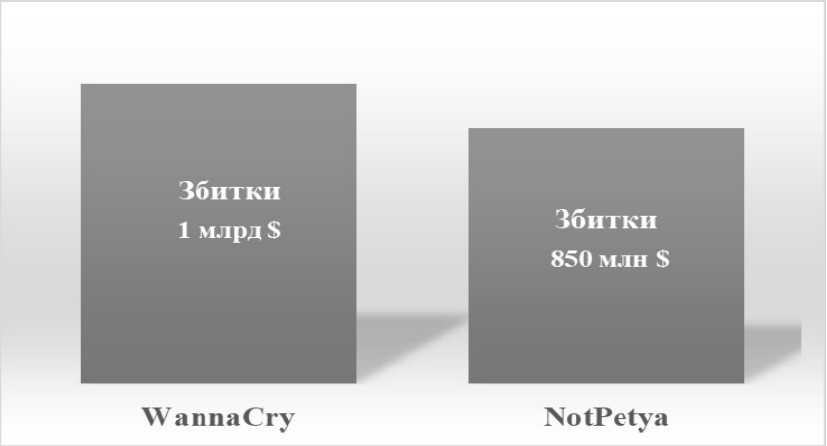

Рис. 1. Найбільші кібератаки в світі за останні роки [складено за джерелами [12, 13]]

Слід зауважити, що процедура підрахунку збитків від кібератак є досить умовною, оскільки в реальності її вивести досить важко. Водночас, якщо виходити із загальних цифр, то кібератаки справляють відчутний економічний збиток. Крім цього, необхідним є визначити, які основні втрати для діяльності підприємства наносять кібератаки:

– втрата інтелектуальної власності;

– втрата бізнес-інформації;

– порушення безперебійності роботи ІТ-систем;

– шкода репутації в результаті атаки;

– втрата персональних даних, які зберігаються у комп'ютерних системах.

Кожна із наведених втрат негативно відображається на діловій активності підприємства, яка взі свого боку є елементом фінансових показників інвестиційної привабливості підприємства. Слід відмітити, що й поняття фінансової безпеки як кількісного і якісного обумовлення фінансового стану, нерозривно пов'язане, як наслідок, з рівнем інвестиційної привабливості підприємства, оскільки інвестор вкладаючи кошти має на меті їх примноження з урахуванням безпечності їх залучення.

Розгляд поняття інвестиційної привабливості як «узагальненої характеристики переваг і недоліків об'єкта інвестування» [14], «сукупності характеристик його виробничої, комерційної, фінансової і управлінської діяльності та особливостей інвестиційного клімату, що свідчать про доцільність здійснення інвестицій в нього» [15], а також «збалансованої системи інтегральних та комплексних показників доцільності вкладання капіталу інвестором в об'єкт інвестування, яка відображає сукупність об'єктивних та суб'єктивних умов, що сприяють або перешкоджають процесу інвестування» [16] є досить багатоаспектним.

У результаті дослідження інвестиційну привабливість підприємства можливо розглядати як певну сукупність показників, які характеризують діяльність підприємства і вказують на доцільність вкладення інвестором вільних коштів з метою отримання вигоди.

Тобто з позиції конкретного інвестора належний рівень фінансової безпеки, який зокрема проявляється у запобіганні втручанням в операційну діяльність підприємства, зменшенні втрат від кіберзагроз шляхом налагодження системи захисту інформаційних систем, впливають на інвестиційну привабливість підприємства. Слід зауважити, що на думку авторів, рівень кіберстійкості підприємств від загроз стане безпосереднім показником, який буде враховуватись в оцінці інвестиційної привабливості підприємства.

ВИСНОВКИ

На сьогодні в Україні в умовах широкого застосування автоматизованих інформаційних систем, заснованих на використанні комп'ютерних і телекомунікаційних засобів, особливої значущості набула проблема кібербезпеки. У результаті проведеного дослідження встановлено, що кібербезпека є значним фактором, який впливає на фінансову безпеку підприємства. З'ясовано, що з поняттям достатнього рівня фінансової безпеки підприємства пов'язаний і необхідний рівень кіберстійкості підприємства, який зі свого боку відображається на фінансових показниках підприємства та його цікавості для потенційних інвесторів.

Необхідний рівень кібербезпеки, забезпечення захисту інформаційних ресурсів підприємств та запобігання несанкціонованому втручанню в операційну діяльність підприємства, позитивно відображається на інвестиційній привабливості, яка відіграє вагому роль у підвищенні конкурентоспроможності підприємства, залученні інвестицій, а також у зміцненні загалом економічної системи країни та гарантуванні захищеності економічних інтересів України.

Список використаних джерел

1. Судакова О.І. Стратегічне управління фінансовою безпекою підприємства. Економічний простір. 2008. № 9. С. 140-148.

2. Кузенко Т.Б. Управление финансовой безопасностью на предприятии. Бизнес-Информ. 2007. № 12 (1). С. 27-29.

3. Бланк И.А. Управление финансовой безопасностью предприятия. Киев: Ника-Центр, Эльга. 2004. 784 с.

4. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. №2163-VIII. Дата оновлення: 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/2163-19

5. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162-169. URL: http://nbuv.gov.ua/UJRN/Infpr_2012_2_24

6. Пантєлєєва Н.М., Романовська Л.В., Романовська М.С. Кіберзагрози в умовах цифрової економіки. Фінансовий простір. 2019. № 1. С. 130-144. URL: http://nbuv.gov.ua/UJRN/Fin_pr_2019_1_10

7. Кіберпростір. URL: https://uk.wikipedia.org/wiki/Кіберпростір

8. Про рішення Ради національної безпеки і оборони

України «Про Стратегію кібербезпеки України». Указ Президента України від 27.01.2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016

9. EY Global Information Security Survey 2018-19 URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf

10. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки «Посилення цифрового середовища проти кібер-загроз» URL: https://www.pwc.com/ua/uk/survey/2018/strengthening-digital-society-against-cyber-shocks.html

11. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak

12. Збитки від глобальних кібератак у світі сягнули $53 мільярдів – МВФ. URL: https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-milardiv-mvf.html

13. Збиток від вірусу WannaCry оцінили в мільярд доларів. URL: https://ms.detector.media/kiberbezpeka/post/18972/2017-05-25-zbitok-vid-virusu-wannacry-otsinili-v-milyard-dolariv/

14. Носова О.В. Інвестиційна привабливість підприємства. Стратегічні пріоритети. 2007. № 1 (12). С. 120–126.

15. Євтушенко С.О. Організаційно-економічні фактори підвищення інвестиційної привабливості промислових підприємств: автореф. ... канд. екон. наук: 08.06.02. Харків, 2001. 20 с.

16. Брюховецька Н.Ю., Хасанова О.В. Оцінка інвестиційної привабливості підприємства: визначення недоліків деяких існуючих методик. Економіка промисловості. 2009. № 1. С. 110-117. URL: http://nbuv.gov.ua/UJRN/econpr_2009_1_17

References

1. Sudakova O.I. Strategic management of enterprise financial security. Economic Scope. 2008. № 9. pp. 140-148. (in Ukrainian)

2. Kuzenko T.B. Management of enterprise financial safety. Biznes-Inform. 2007. № 12(1). pp. 27-29 (in Russian)

3. Blank I.A. The financial management enterprise security. Kyiv: Nika-Tsentr, Elga. 2004. 784 p. (in Russian)

4. On Main Principles of Maintaining Cybersecurity of Ukraine: Law of Ukraine of October 05, 2017 № 2163-VIII. Update date: 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian).

5. Furashev V.M. Cyberspace and information space, cybersecurity and information security: intension, definition, differences. Information and Law. 2012. № 2. pp. 162-169. URL: http://nbuv.gov.ua/UJRN/Infpr_2012_2_24 (in Ukrainian).

6. Pantielieieva N.M., Romanovska L.V., Romanovska M.S. Cyberthreats in the digital economy. Financial Space. 2019. № 1. pp. 130-144. URL: http://nbuv.gov.ua/UJRN/Fin_pr_2019_1_10 (in Ukrainian)

7. Cyberspace. URL: https://uk.wikipedia.org/wiki/Кіберпростір (in Ukrainian).

8. On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 «On the Cyber Security Strategy of Ukraine»: Presidential Decree. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (in Ukrainian)

9. EY Global Information Security Survey 2018-19 URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf

10. Key findings from The Global State of Information Security Survey 2018. «Strengthening digital society against cyber shocks». URL: https://www.pwc.com/ua/uk/survey/2018/strengthening-digital-society-against-cyber-shocks.html (in Ukrainian)

11. Pill from hackers: how business protects itself from cyberattacks. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak (in Ukrainian)

12. Losses from global cyberattacks in the world reached $53 billion - the IMF. URL: https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-milardiv-mvf.html (in Ukrainian)

13. The damage from the WannaCry virus was estimated at a billion dollars. URL: https://ms.detector.media/kiberbezpeka/post/18972/2017-05-25-zbitok-vid-virusu-wannacry-otsinili-v-milyard-dolariv/ (in Ukrainian)

14. Nosova O.V. Investment attractiveness of enterprise. Strategic Priorities. 2007. № 1 (12). pp. 120–126. (in Ukrainian)

15. Yevtushenko S.O. Economical and organization factors of productive enterprise investment appeal: abstract diss. ... cand. econ. sciences: 08.06.02. Kharkiv, 2001. 20 p. (in Ukrainian)

16. Brukhovetska N.Y., Khasanova O.V. Assessment of the investment attractiveness of the enterprise: determination of disadvantages of some existing methods. Economy of Industry. 2009. № 1. pp. 110-117. URL: http://nbuv.gov.ua/UJRN/econpr_2009_1_17 (in Ukrainian)