УДК 368:004]368.71
DOI: 10.25140/2411-5215-2020-1(21)-183-196

Максим Дубина, Ірина Середюк, Наталія Білоус

РОЛЬ КІБЕРСТРАХУВАННЯ В СИСТЕМІ РИЗИК-МЕНЕДЖМЕНТУ БАНКІВСЬКИХ УСТАНОВ

Максим Дубина, Ирина Середюк, Наталья Белоус

РОЛЬ КИБЕРСТРАХОВАНИЯ В СИСТЕМЕ РИСК-МЕНЕДЖМЕНТА БАНКОВСКИХ УЧРЕЖДЕНИЙ

Maksym Dubyna, Iryna Seredyuk, Natalia Bilous

THE ROLE OF CYBER INSURANCE IN THE RISK MANAGEMENT SYSTEM OF BANKING INSTITUTIONS

У статті проведено дослідження ролі кіберстрахування в розвитку систем ризик-менеджменту банківських установ, а саме конкретизовано сутність такої системи, визначено умови виникнення кіберризиків та їхні потенційні можливості до формування загроз діяльності банківських установ. Значна увага приділена аналізу наслідків виникнення та дії кібератак у діяльності цих установ, досліджено сутність кіберстрахування як методу мінімізації втрат від таких впливів, конкретизовано особливості надання послуг страхування кіберризиків страховими компаніями комерційним банкам. Також розкрито сучасні тенденції витрат організацій на проведення заходів щодо забезпечення власної кібербезпеки та придбання відповідних страхових продуктів, уточнено заходи підвищення безпеки банківських установ на основі удосконалення їхніх внутрішніх систем контролю та фінансової безпеки.

Ключові слова: *кіберризик; цифровізація; банківська система; кіберстрахування; діджиталізація; кібератака.*
Табл.: 1. Рис.: 5. Бібл.: 25.

В статье проведено исследование роли киберстрахования в развитии систем риск-менеджмента банковских учреждений, а именно конкретизирована сущность такой системы, определены условия возникновения киберрисков и их потенциальные возможности для формирования угроз деятельности банковских учреждений. Значительное внимание уделено анализу последствий возникновения и действия кибератак в деятельности этих учреждений, исследована сущность кіберстрахування как метода минимизации потерь от таких воздействий, конкретизированы особенности предоставления услуг страхования киберрисков страховыми компаниями коммерческим банкам. Также раскрыты современные тенденции расходов организаций на проведение мероприятий по обеспечению собственной кибербезопасности и приобретение соответствующих страховых продуктов, уточнены меры повышения безопасности банковских учреждений на основе совершенствования их внутренних систем контроля и финансовой безопасности.

Ключевые слова: *киберриск; цифровизация; банковская система; киберстрахование; диджитализация; кибератака.*
Табл.: 1. Рис.: 5. Библ.: 25.

Within the article, the role of cyber insurance in the development of risk management systems of banking institutions is researched, namely, the essence of this system is specified, conditions of cyber risks and their potential for threats to banking institutions are identified. Considerable attention is paid to the analysis of the consequences and actions of cyber attacks in the activities of these institutions, the essence of cyber insurance as a method of minimizing losses from such influences is studied, peculiarities of providing cyber risk insurance services by insurance companies to commercial banks are specified. In addition, current trends as for the costs of organizations to take measures to ensure their own cybersecurity and purchase of appropriate insurance products are revealed, measures to improve security of banking institutions based on improving their internal control systems and financial security are specified.

Keywords: *cyber risk; digitalization; banking system; cyber insurance; digitalization; cyber attack.*
Table: 1. Fig: 5. References: 25.
JEL Classification: G22; G21

Постановка проблеми. Банківська система є ключовою складовою розвитку національної економіки. Діяльність банківських установ відіграє одну з ключових ролей у процесах кредитування та інвестування, які є об'єктивно необхідними для розбудови господарства країни. Це відбувається за допомогою трансформації тимчасово вільних коштів економічних суб'єктів у фінансові ресурси, які є необхідними для активізації, насамперед, діяльності суб'єктів підприємницької діяльності. Стабільність функціонування банківської системи є важливою з позиції забезпечення ефективного функціонування окремих галузей та формування умов для стабільного економічного зростання в країні.

Отже, стійкий розвиток банківських установ, їхня спроможність протидіяти впливу непередбачуваних екзогенних та ендогенних факторів є важливою умовою для створення сприятливого економічного простору розвитку господарства країни. Банківській системі притаманна мультиплікативна властивість поширювати внутрішні системні

проблеми у власному функціонуванні на роботу інших економічних суб'єктів. Саме тому велику увагу органи державної влади приділяють формуванню умов для забезпечення стійкості банківської системи, підтримці належного рівня її ліквідності.

Проте банківська система розвивається в зовнішньому, досить мінливому економічному середовищі, що продукує постійно нові виклики та загрози для роботи банків. Відповідно для цих установ існує об'єктивна умова формування дієвих систем ризик-менеджменту для виявлення та протидії ризикам різної природи, які можуть загрожувати безпечній роботі цих установ.

На сьогодні вся сфера фінансових відносин перебуває в трансформаційному процесі власного оновлення, розвитку та зміни усталених моделей надання фінансових послуг та роботи самих фінансових установ. Процеси діджиталізації, прискорення темпів впровадження новітніх інформаційних, фінансових технологій змінюють базові засади розвитку й банківської системи загалом. Такі зміни досить часто призводять до виникнення нових загроз, перешкод для подальшого розвитку банківських установ. Це вимагає від їхніх власників та топменеджерів відповідного реагування і обумовлює формування нових вимог і до побудови системи ризик-менеджменту в цих установах.

Процеси діджиталізації передусім призвели до створення нових загроз у віртуальному просторі, що безпосередньо пов'язаний із розробкою та впровадженням нових технологій, які використовують потенціал мережі Інтернет, сучасних інформаційних продуктів. Відповідно це призвело до вже перманентного виникнення кібератак, які зумовлюють створення нових кіберризиків для роботи комерційних банків. Це, у свою чергу, також вимагає пошуку нових механізмів, інструментів для їх попередження та протидії.

Страхування як один із найбільш дієвих способів управління ризиками банківських установ також може бути корисним і сприяти зростанню стабільності їхньої роботи. Страхові компанії вже розробили та пропонують фінансовим установам відповідні послуги щодо страхування власної діяльності від наслідків кібератак, пропонують нові інструменти зниження власних втрат банківськими установами. Відповідно, вже на сьогодні зародився і досить швидко розвивається ринок кіберстрахування в усьому світі, що обумовлює зростання попиту з боку фінансових установ, включаючи банки, на відповідні страхові послуги. Таким чином, це актуалізує питання щодо проведення нових досліджень для поглиблення теоретичних, методологічних та прикладних положень розвитку страхування в країні та обґрунтування його ролі в управління кіберризиками банківських установ.

Аналіз останніх досліджень та публікацій. Актуальність розвитку банківських установ в епоху діджиталізації, впровадження нових технологій та протидія новим ризикам у діяльності цих фінансових посередників, удосконалення функціонування їхніх систем ризик-менеджменту обумовили нові дослідження в цій сфері. До науковців, які активно займаються вивченням окреслених питань, варто віднести таких: І. Бєлова, В. Бобиль, Т. Васильєва, Д. Гладких, Ж. Довгань, С. Євсєєв, Л. Жердецька, О. Криклій, Л. Кльоба, Л. Примостка, Н. Ткаченко, Н. Швець, Alina Teodora Ciuhureanu, Nicolae Baltes, Okan Şafakli, Pelin Yaylali, Turgut Türsoy.

Питання пошуку нових інструментів попередження кіберризиків та використання для цього страхування розглядаються в працях таких дослідників: О. Гудзь, Н. Нагайчук, Л. Селіверстова, A. Marotta, R. Böhme, Allen G. Schwartz, S. Romanosky, L. Ablon, A. Kuehn, T Jones, Laura A. Odell, J. Corbin Fauntleroy, Ryan R. Wagner, Antoine Bouveret, İsmail Yıldırım.

Виділення недосліджених частин загальної проблеми. Однак попри наявність значної кількості наукових праць у сфері кіберстрахування, нових теоретичних та прикладних досліджень, активне впровадження сучасних інноваційних технологій у роботу

банківських установ, швидка зміна моделей їхньої роботи та способів надання послуг, виникнення нових ризиків у цій сфері обумовлюють необхідність проведення додаткових досліджень з метою виявлення та обґрунтування особливостей покращення роботи систем ризик-менеджменту в банківських установах, використання страхування в процесі управління кіберризиками цими фінансовими установами.

Мета статті. Метою статті є дослідження ролі кіберстрахування в системі управління кіберризиками банківських установ, обґрунтування сучасних тенденцій у забезпеченні їхньої стабільної роботи в епоху діджиталізації ринків фінансових послуг.

Виклад основного матеріалу. Система ризик-менеджменту є невід'ємною складовою діяльності банківських установ, оскільки їх функціонування безпосередньо завжди пов'язано із сукупністю фінансових ризиків. Саме ефективна організація такої системи, використання сучасних методів та інструментів управління окресленими ризиками сприяють стабільності банків, забезпеченню їхньої прибуткової діяльності в довгостроковій перспективі. Перманентні кризи на фінансовому ринку, які ми спостерігаємо протягом останніх десяти років, лише підтверджують важливість здійснення якісного ризик-менеджменту всіма фінансовими установами, особливо банками, враховуючи обсяги їхніх фінансових операцій та спроможність негативно впливати на функціонування всієї банківської системи в разі виникнення труднощів у роботі будь-якої з таких установ.

Загалом система ризик-менеджменту являє собою сукупність різних методів, інструментів, організаційних центрів, які взаємодіють між собою з метою ідентифікації, аналізу, протидії ризикам різної природи та підвищенню загального рівня стабільності роботи суб'єктів господарювання [1; 2; 25]. Відповідно в банківських установах такі системи створюються з метою організації всього процесу управління фінансовими ризиками, забезпечення стабільності роботи зазначених установ. Проте, враховуючи нові виклики, які на сьогодні формуються в межах фінансових систем і обумовлені новими процесами цифровізації сектору фінансових послуг, системи ризик-менеджменту банківських установ також змінюються, впроваджуються методи та інструменти управління новими загрозами, включаючи кіберризики.

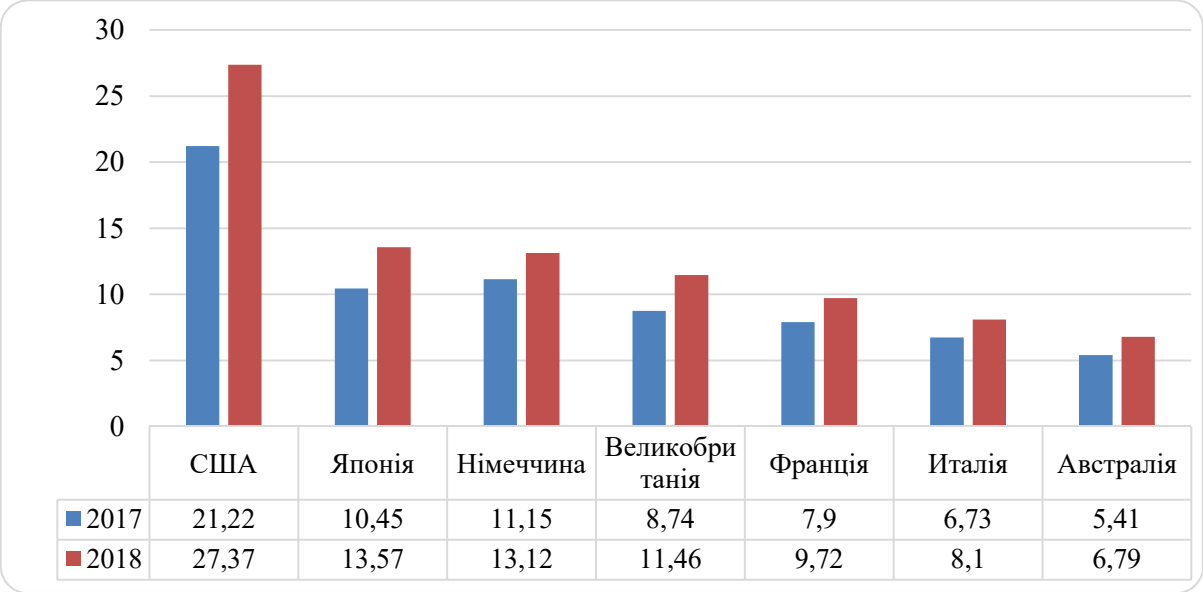
Злочинність у кіберпросторі стала однією з головних проблем сучасного світу інформаційних технологій. Українська банківська система відчула весь масштаб кіберзагроз після атаки вірусу Petya, від якого потерпіли мінімум 22 банків. І хоча після Petya банки почали посилювати свою кібербезпеку, у багатьох із них керівництво розглядає кібератаки як другорядні, не основні ризики, які не спроможні завдати значної, непоправної шкоди для роботи банківських установ. Однак поступово реальність окреслених загроз змінюється, і кіберризики вже стали невід'ємною частиною функціонування банків у всьому світі.

Протягом останніх років кібератаки почастішали, а наслідки від їхнього впливу стали глобальнішими та більш витратними для фінансових установ, зокрема й комерційні банки. Кібератаки, такі як відключення платіжних систем вірусами Petya та WannaCry, продемонстрували здатність окремих осіб або їх груп здійснювати негативний вплив на роботу банківських установ, порушувати функціонування їхніх операційних систем, програмного забезпечення. Такі кібератаки були виявлені в понад 150 країн світу й завдали збитків на 12 млрд дол. Банківські установи різного масштабу та географічного розташування в усьому світі зазнали фінансових, репутаційних та регуляторних наслідків кіберзлочинності. Кібератаки повільно змінюють свої схеми нападу з метою використання сторонніх партнерів та ланцюгів постачання, щоб отримати доступ до цільових систем [22].

Враховуючи те, що у світі у сфері фінансових послуг залежність роботи банків від мережі Інтернет та впровадження фінансових технологій розширюється, відповідно 68 % керівників банківських установ заявляють, що їхні ризики в галузі кібербезпеки

також зростають. Інформація Європейської ради системного ризику «ESRB» свідчить, що витрати на ліквідацію наслідків від різних кіберінцидентів у 2018 році для світової економіки становили від 45 млрд дол. до 654 млрд дол. [4]. За підрахунками, середня вартість кіберінцидентів за останні п'ять років зросла на 72 %. Прогнозовано, що компанії ставатимуть жертвами нападу зловмисних програм кожні 11 секунд до 2021 року [19]. За даними Світового економічного форуму кібератаки та шахрайство або крадіжки даних нині є двома з перших п'яти ризиків, з якими найчастіше стикаються генеральні директори банківських установ [23].

Глобальна консалтингова компанія Accenture провела дослідження вартості кіберзлочинності в 11 країнах, у 16 галузях у 2017–2018 роках (рис. 1).



	США	Японія	Німеччина	Великобританія	Франція	Італія	Австралія
2017	21,22	10,45	11,15	8,74	7,9	6,73	5,41
2018	27,37	13,57	13,12	11,46	9,72	8,1	6,79

Рис. 1. Середньорічна вартість кіберзлочинності в США, Японії, Австралії та країнах ЄС у 2017–2018 рр., млн дол. США

Джерело: складено авторами на основі [22].

Згідно з даними дослідження, США очолює список країн із найбільшою середньорічною вартістю кіберзлочинності, яка зросла на 29 % у 2018 році та становила 27,4 млн дол. США. Але найбільше зростання витрат від кіберзлочинності спостерігалося у Великобританії, де їх приріст становив 31 %, а це 11,5 млн дол. США. В Японії витрати на покриття збитків від кіберзлочинності збільшилися у 2018 році на 30 % і становили 13,6 млн дол. США. Темп зростання витрат, пов'язаних із покриттям втрат від кібератак, у Німеччині у 2018 році значно знизився. Це зумовлено впровадженням компаніями цієї країні нових технологій для запобігання таким атакам та зниження їхнього впливу на стабільність розвитку організацій.

На рис. 2 представлено інформацію про обсяг збитків, які зазначає суб'єкт господарювання від окремих типів кібератак.

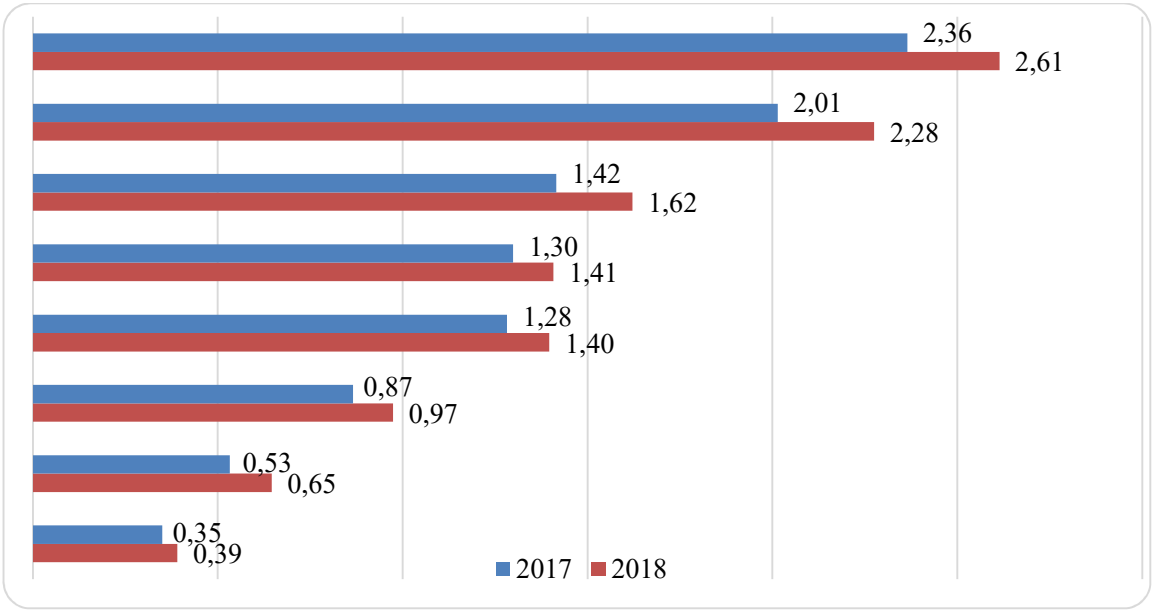


Рис. 2. Середньорічна вартість кіберзлочинності за типом нападу у 2017–2018 рр., млн дол. США

Джерело: складено авторами на основі [22].

Таким чином, аналіз інформації рис. 2 свідчить про те, що найбільше збитків організації отримують від використання зловмисниками програмного забезпечення. Середньорічна вартість від таких атак становила у 2018 році – 2,61 млн дол. США. та збільшилася в порівнянні з даними 2017 року. Також значні збитки підприємства отримують від вебатак. У 2018 році – 2,28 млн. дол. США у розрахунку на один випадок. Загрози від інсайдерів та працівників зросли на 14,1 %. При цьому ботнети займають найменшу частку серед втрат від кіберзлочинності.

Розглянемо збитки від кіберзлочинів у розрізі окремих секторів та галузей національного господарства у 2017–2018 роках. На рис. 3 наведено відповідну інформацію.

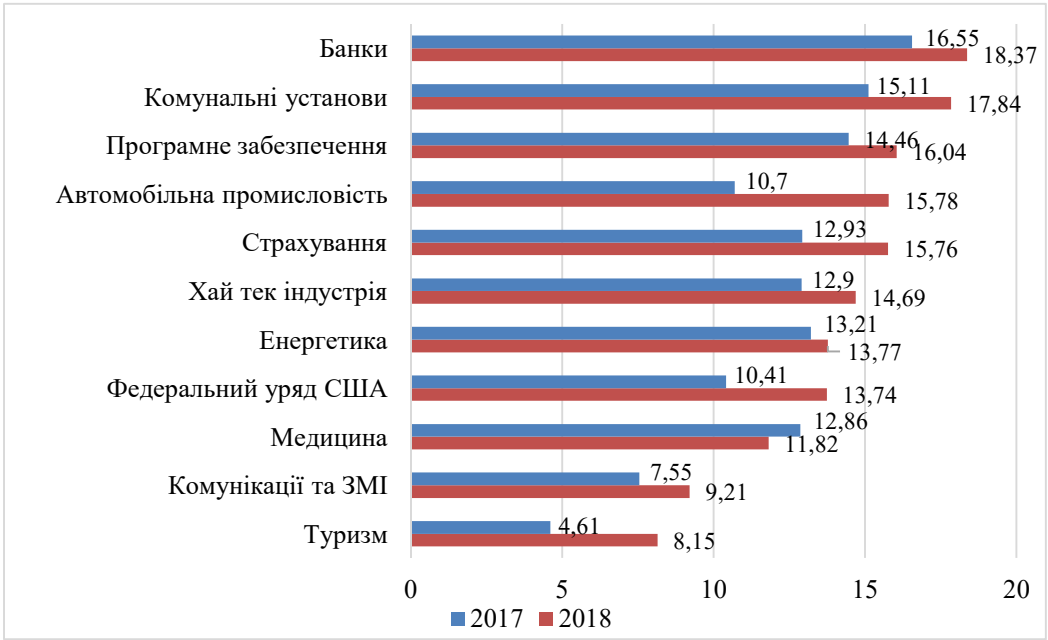


Рис. 3. Середньорічна вартість кіберзлочинності за галузями у 2017–2018 рр., млн дол. США

Джерело: складено авторами на основі [22].

Отже, найбільших втрат від кіберзлочинності на сьогодні зазнають банківські установи, що зумовлено специфікою їхньої роботи, масштабним використанням сучасних технологій для покращення якості надання фінансових послуг. У 2018 році банки отримали в середньому збитків у розмірі 18,37 млн дол. США, що більше аналогічного показника 2017 року на 1,82 млн дол. США. Прогнозуємо й подальше зростання кількості кібератак на роботу цих установ та зростання витрат на подолання їхніх наслідків. Це ще раз підтверджує важливість формування в межах банківських систем ефективно діючих систем ризик-менеджменту, які б були спроможні визначати такі ризики, аналізувати наслідки їхніх впливів та пропонувати технології мінімізації такого впливу на стабільність функціонування цих установ.

Також дані рис. 3 свідчать про досить суттєве зростання втрат від кіберзлочинності у 2017–2018 роках. Якщо у 2017 році цей показник становив 12,93 млн дол. США, то вже у 2019 році – 15,76 млн дол. США. Варто також зазначити і швидкі темпи зростання середньорічної вартості кіберзлочинності в комунальних установах (16,0 %), автомобільній промисловості (67,8 %).

На сьогодні багато співробітників банківських установ часто є першопричиною успішності кібератак, що підтвердило опитування керівників у провідних країнах світу консалтинговою компанією Accenture [22]. Забезпечення постійного навчання та підвищення кваліфікації спеціалістів (наприклад, фішинг-тестів) є надзвичайно важливим для запобігання шахрайським діям. Співробітники банку повинні розуміти, які електронні листи можна відкривати, а про які листи краще інформувати службу безпеки [22]. У IV кварталі 2019 року члени APWG OpSec Security встановили, що вебпошти залишаються найчастішими об'єктами фішингу. Наступними за популярністю нападів є платіжні системи (19,8 %) та фінансова галузь (19,4 %). Атаки на хмарні вебсайти для зберігання файлів, телекомунікацію та логістику залишалися менш популярними – від 3 до 3,5 % (рис. 4).

Рис. 4. Інтернет-галузі, на які найбільше націлені фішинг-атаки станом на IV квартал 2019 року

Джерело: складено авторами на основі [20].

З огляду на вищезазначене можна зробити висновки з наведеного аналітичного матеріалу, що фінансова сфера й надалі буде залишатися найбільш привабливим сектором для здійснення кібератак на діяльність банківських установ, а тому питання удосконалення роботи системи ризик-менеджменту залишатимуться актуальними і надалі. Також важливим і обов'язковим компонентом підвищення якості цієї системи стане використання нових методів, технологій та інновацій управління кіберризиками. Розглянемо більш детально сутність цієї групи ризиків.

Взагалі сутність дефініції «кіберризик» чітко не визначена в науковій літературі. Здебільшого вчені розглядають під цією групою ризиків усі деструктивні процеси, виникнення та розвиток яких пов'язаний із використанням інформаційних технологій, програмного забезпечення. Наприклад, С. Волосович, Л. Клапків зауважують, що «у широкому значенні кіберризик – це ймовірність загрози інтерактивним цифровим мережам, що використовуються для передачі, модифікації та зберігання інформації (кіберпростору). У вузькому значенні кіберризики пов'язані з операційними загрозами інформаційним та технологічним активам, які негативно впливають на конфіденційність, доступність та цілісність інформації або інформаційної системи. Кіберризик – це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі» [3]. У свою чергу, Н. Нагайчук констатує, що «кіберризик – це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення, як в локальних мережах, так і в глобальній Інтернет-мережі; в розрахунково-платіжних системах, системах інтернет-торгівлі, промислових системах управління; а також ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних» [7]. А. Амухопадхей, Д. Саха, Б. Чакрабарті, А. Маханті та А. Подер пропонують таке трактування сутності «кіберризику»: «ризик, пов'язаний зі шкідливими електронними подіями, які викликають порушення ділових відносин та грошових втрат» [12]. С. Бієнер, М. Елінг та Дж. Вірфс зауважують, що «кіберризик – ризик, який призводить до невдачі інформаційних систем; кіберризики належать до галузі, яка створюється як цифрова мережа й використовується для зберігання, зміни та передачі інформації» [18].

На наше переконання, кіберризик варто розглядати як ймовірність настання негативних наслідків від стороннього втручання в роботу інформаційних систем, програмного забезпечення, цифрових та іншим електронних пристроїв та технологій, які призводять до порушення нормального функціонування об'єктів нападу, формують збитки від їх використання.

Страхування є традиційним способом мінімізації витрат від виникнення непередбачуваних обставин, які призводять до погіршення стану роботи банківських установ. Нині банки досить часто використовують послуги страхових компаній для зниження власних ризиків у різних сферах своєї роботи. Проте у сфері протидії негативному впливу від кібератак, страхування для компенсації витрат від їхнього деструктивного впливу використовується не так активно.

Розвиток кіберстрахування очікується в майбутньому і, на думку експертів, цей сегмент стане невід'ємно частиною світового ринку страхових послуг. Зауважимо, що у 2018 році у фінансовому секторі було викрито загалом 3,55 млн особистих даних. Витрати на кібератаки досить високі для сектору фінансових послуг. Глобальні кіберзлочини спричинили в середньому 18,37 млн дол. США щорічних збитків для галузі фінансових послуг – найвищий середній показник серед усіх галузей. Тому європейські та американські банки та інші фінансові установи дедалі частіше сприймають кіберстрахування як необхідність для захисту електронних даних [9]. Частка компаній, які не усвідомлюють цей ризик, також зменшується, що свідчить про те, що актуальність використання цього методу мінімізації витрат зростає і в майбутньому спостерігатиметься збільшення попиту на відповідні страхові продукти.

За даними аудиторської компанії PwC, близько 90 % від усього світового ринку кіберстрахування купують американські компанії, підкреслюючи розмір можливостей для подальшого розширення ринку за межами країни, і лише приблизно від 5 до 9 % базується в Європі. Наприклад, у Великобританії лише 2 % компаній мають автономне кіберстрахування. Навіть на більш розвиненому ринку США лише близько третини компаній мають певну форму кіберпокриття, тоді як більшість їхніх керівників тільки починають замислюватися над цим питанням [8]. Враховуючи цю асиметрію, більшість звітів та опитувань у сфері використання страхування ризиків, пов'язаних із кібершахрайством, стосуються розвитку, насамперед, страхового ринку США та провідних країн ЄС. За даними Fitch Ratings, галузь кіберстрахування в США зросла на 8 % у 2018 році, тобто приблизно до 2 млрд дол. виплат [24]. Страхові компанії США надають значну кількість програм страхування кіберризиків, до яких варто віднести такі: ризик втрати інформації під час злому паролю доступу або внаслідок DDoS-атаки, ризик фінансових втрат через викрадення та розголошення персональних даних та іншої інформації, ризик фінансових втрат через порушення роботи комп'ютерних систем, ризик фінансових втрат від фішингових атак, ризик фінансових втрат від кібершантажу або вірусного блокування комп'ютерних систем.

Розглянемо більш докладно сутність кіберстрахування як економічної категорії. Деякі вчені зауважують, що «кіберстрахування – це широкий термін для пояснення страхових полісів, які гарантують виплати втрат в результаті комп'ютерної атаки або несправності систем інформаційних технологій фірми» [21]. R. Bohme, G. Schwartz констатують, що «кіберстрахування – це передача фінансових ризиків, які пов'язані з мережевими та комп'ютерними атаками, третім особам» [14]. Laura A. Odell, J. Corbin Fauntleroy, Ryan R. Wagner надають таке визначення сутності кіберстрахування: продукт передачі ризику корпораціям, який дозволяє зменшити втрати через проблеми з інформаційними технологіями (IT) [16, с. 1]. Наприклад, Л. Селіверстова та Д. Трухан зазначають, що «кіберстрахування є динамічним сегментом глобального ринку страхових послуг. Безсумнівно, цей вид страхування розглядається як метод управління ризиками та захисту від різних загроз, що виникають при здійсненні електронної комерції» [9, с. 25]. О. Гудзь зауважує, що «кіберстрахування – це страховий продукт, який захищає економічні суб'єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет - мережі, ІКТ-інфраструктури та діяльності у кібер-просторі» [3, с. 5].

Таким чином, можна стверджувати, що кіберстрахування – це відносини, що виникають між страховиком та страхувальником у процесі передачі на певних умовах страховику фінансових ризиків, які пов'язані з порушенням роботи інформаційних систем або програмного забезпечення страхувальника в результаті зовнішнього втручання в їхню роботу. Конкретизуємо особливості кіберстрахування як окремого виду мінімізації втрат від кібератак. Їх перелік наведено в таблиці.

Таблиця

Особливості страхування кіберризиків

Риса (особливість)	**Характеристика**
1	2
Брак досвіду страховиків і відсутність відповідних стандартів	кіберстрахування – це новий вид страхування, і страховики ще не мають чіткої стандартизованої процедури, яким чином визначати ймовірність настання страхових випадків, як оцінювати збитки, як унеможливити зловживання з боку організацій, що зазнали відповідних втрат
Постійний швидкий розвиток інформаційних систем	комп'ютерні системи швидко еволюціонують, з'являються нові технології, які можуть змінювати природу кіберризиків, підвищувати їхній деструктивний вплив. Техніки і прийоми, які використовують кіберзлочинці, постійно удосконалюють і вони є непередбачуваними

Закінчення табл.

1	2
Інформаційна асиметрія	існує певна межа доступу страхової компанії до інформації страхувальника, що обумовлено, наприклад, банківською таємницею або корпоративними конфіденційними даними, що ускладнює можливість правильної оцінки вартості страхових продуктів, визначення компенсацій у разі настання страхових подій
Взаємозалежність систем безпеки організацій	рівень захисту однієї організації може бути залежним від ефективної роботи такої ж системи в організації-партнера, замовника, контрагента, оскільки окремі кіберзагрози можуть проникати до інформаційних систем через канали інших, афільованих компаній
Недостатність статистичних та аналітичних даних	існує у сфері кіберстрахування дефіцит інформації про кількість атак, втрати компаній від них, оскільки організації намагаються не афішувати ці аспекти власної діяльності, а самостійно їх вирішувати. Це знову ускладнює роботу страховим компаніям, оскільки не дозволяє їм оперувати актуальною та реальною інформацією про даний вид ризиків
Проблеми з визначенням покриття	інколи досить складно чітко конкретизувати ті ризики, від яких страхувальник бажає застрахуватися, складніше встановити наслідки від кібератак, оскільки це впливає на вартість страхового продукту
Винятки та обмеження	враховуючи досить широкий спектр різних подій, які прийнято називати кібератаками, страхові компанії в договорах досить часто прописують значну кількість винятків та обмежень, коли відшкодування не буде здійснено
Визначення центра відповідальність	виникнення кіберризиків та негативних наслідків від їх проявів вимагає чіткого встановлення відповідальних за їх виникнення, оскільки, з одного боку, це можуть бути власники організації, яка зазнала негативного впливу, її відповідальні особи, а з іншого – розробники програмного забезпечення, компанії, які надають інформаційні послуги
Час для пред'явлення претензій	значна кількість атак відбуваються непоміченими. Порушення в роботі системи можуть бути виявлені вже після нападу. Крім того, деякі атаки є надзвичайно тривалими (наприклад, напади можуть зайняти кілька місяців). Питання про те, яким чином страховики повинні відшкодувати витрати, залишається відкритим

Джерело: [5; 6; 10; 13; 15; 17].

Активний розвиток кіберстрахування у світі зумовлений постійним зростанням кібератак та збільшенням обсягів збитків, як отримують від них організації. У великій кількості корпорацій, які мають складну організаційну структуру, значну кількість структурних підрозділів кіберризики розглядають як один із найбільш небезпечних деструктивних чинників, що впливає на стабільність їхньої роботи та обсяг отриманого прибутку. Відповідно, такі компанії приділяють важливу увагу протидії таким атакам, впроваджують нові системи їх запобігання, кібербезпеки, що вимагає значних інвестиційних ресурсів. На рис. 5 представлено дані про витрати суб'єктів господарювання, що були здійснені на підвищення рівня кібербезпеки та придбання полісів кіберстрахування в усьому світі з 2015 по 2019 рік.

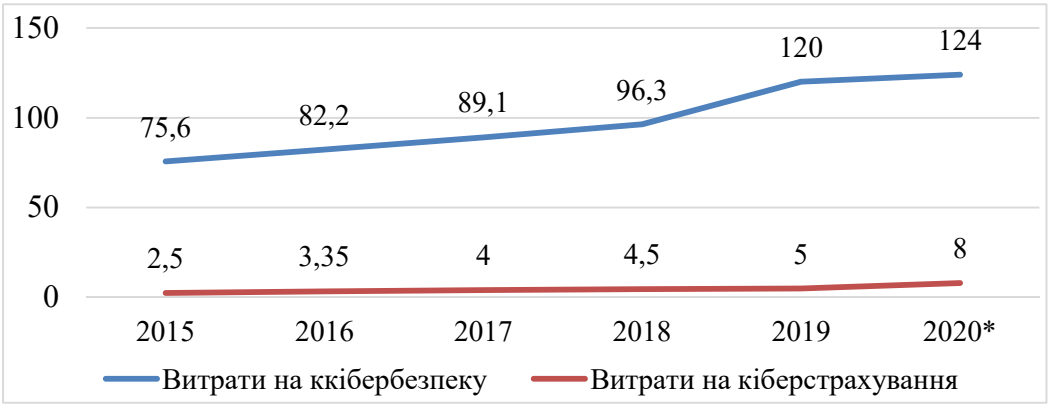


Рис. 5. Щорічні витрати на кібербезпеку та кіберстрахування в усьому світі у 2015–2019 рр., млрд дол. США

Джерело: [11].

Таким чином, дані рис. 5 свідчать про постійне зростання витрат на окреслені заходи протягом усього періоду, що аналізується. Якщо у 2015 році витрати на заходи для забезпечення кібербезпеки становили 75,6 млрд дол. США, то вже у 2019 році – 120 млрд дол. США, а за прогнозом у 2020 – 124 млрд дол. США. Фактично за п'ять років зростання становило понад 44 млрд дол. США. Це лише свідчить про рівень зростання загроз від кібератак та збільшення збитків від їхнього впливу [11].

Поступово також збільшуються витрати й на придбання полісів кіберстрахування. Якщо у 2015 році їх вартість становила всього 2,5 млрд дол. США, то вже у 2019 році – збільшилася вдвічі – до 5 млрд дол. США, а за прогнозами у 2020 році очікується значний розвиток цього виду страхування, а обсяги страхових премій від нього повинні перевищити 8,0 млрд дол. США.

Інформація рис. 5 також дозволяє зробити висновок, що у 2015-2019 роках більшість компаній у всьому світі намагалася самостійно вирішувати проблеми щодо захисту від кібератак, що підтверджується лише обсягами тих ресурсів, які вони вкладали у власну безпеку. Проте поступово на сьогодні відбувається і розвиток кіберстрахування як одного зі способів зниження витрат від кіберризиків. Якщо проаналізувати тренд витрат на кібербезпеку, то в середньому кожного року компанії витрачали на 6-7 млрд дол. США більше, ніж у попередньому році. Однак за даними на 2020 рік цей показник прогнозовано вже на рівні 4,0 млрд дол. США.

Кібератаки є основним фактором ризику як для приватних, так і для державних банків. Уже на сьогодні страховими компаніями розроблено нові страхові продукти для мінімізації можливих втрат від кібератак в різних галузях, що мають назву «Страхування відновлення даних», «Страхування захисту даних», «Кіберстрахування» та «Страхування кібервідповідальності».

Отже, можна спрогнозувати, що попит на окреслені продукти страхових компаній, зокрема з боку банківських установ буде зростати, що зумовлено специфікою їхньої діяльності, вразливістю до кібератак різних типів. Для покращення захисту цих установ від окреслених загроз необхідно також:

1) підвищувати обізнаність працівників банківських установ щодо можливостей втручання в їх роботу ззовні, види кіберризиків та наслідки від їх впливу;

2) забезпечувати належний рівень збереження конфіденційності корпоративної інформації серед працівників, чітка регламентація тих даних, які не підлягають розголошенню;

3) підвищення ефективності роботи інформаційних систем у банківських установах, мінімізації взаємодії працівників із зовнішніми джерелами інформації в мережі Інтернет;

4) чітка регламентація доступу працівників до відкритих джерел даних у мережі Інтернет, визначення тих осіб, які цього не мають права робити;

5) роз'яснення серед працівників алгоритму дій, якщо вони запідозрили втручання в роботу інформаційної системи банку ззовні;

6) організація резервного копіювання даних про клієнтів, роботу банківських установ, що дозволяє провести її відновлення в разі втрати через кібератаки;

7) впровадження внутрішньої системи контролю за роботою працівників та дотримання ними протоколів безпеки банківської установи.

Більшість перерахованих заходів на сьогодні банківські установи вже впроваджують з метою запобігання різним загрозам та втраті власної репутації. Проте в багатьох таких установах такі заходи мають фрагментарний характер і не є систематичними.

На наш погляд, забезпечити найкращий захист від кібератак на сьогодні можна банківськими установами лише через поєднання створення власних систем запобігання відповідним ризикам та використання кіберстрахування. Саме такий синтез дозволяє більш системно виокремити ті ризики, які доцільно застрахувати, та ті, управління якими краще

виконувати власними силами через певні обмежувальні чинники (конфіденційність даних, банківська таємниця тощо). Також варто розуміти, що кіберстрахування теж не є 100 % гарантією захисту від кібератак для банків. Самі страхові компанії також піддаються впливу ззовні й це може призводити до втрати даних цих компаній і частково негативно впливати також на репутацію їхніх клієнтів, включаючи банківські установи.

Висновки та пропозиції. Отже, в межах статті було розглянуто питання щодо теоретичного та прикладного обґрунтування сутності кіберстрахування та особливостей його розвитку у світі. Варто констатувати, що дослідження дійсно підтвердила існування об'єктивних передумов для розвитку досліджуваного виду страхування в подальшому та необхідності зміни банківськими установами сформованих систем ризик-менеджменту.

У статті констатовано, що виклики, які виникають перед банківською системою в результатів діджиталізації всього ринку фінансових послуг, продукують також і нові загрози для роботи банківських установ. Постійні кібератаки на роботу цих установ стають невід'ємною частиною їхньої роботи. Відповідно виникає потреба в управління такими ризиками, що обґрунтовує пошук нових методів та інструментів ризик-менеджменту, до яких варто віднести й кіберстрахування.

У роботі вагому увагу приділено обґрунтуванню сутності кіберстрахування, особливостей його провадження. Також з'ясовано, що за останніми тенденціями дедалі більше банківських установ почали звертатися саме до страхових компаній з метою зниження власних витрат від наслідків впливу кібератак на їхню діяльність. Зокрема, визначено, що страхові компанії швидко почали адаптуватися до ринкових потреб і вже розробили спектр страхових продуктів для різних типів суб'єктів господарювання.

Однак детальний аналіз особливостей функціонування банківської системи дає підстави стверджувати, що для цих установ найкращим способом управління кіберризиками є гармонійне поєднання побудови власних систем забезпечення кібербезпеки з використанням послуг страхових компаній. Саме синтез таких підходів дає найкращий результат для забезпечення ефективного функціонування систем ризик-менеджменту та загалом стійкості цих установ.

Актуальними на сьогодні залишаються також питання дослідження наслідків впливу кібератак на роботу банківських установ, включаючи фінансові, організаційні та репутаційні втрати, особливостей фінансового забезпечення впровадження механізмів підвищення рівня кібербезпеки та ефективної роботи системи ризик-менеджменту.

Список використаних джерел

1. Гладких Д. М. Забезпечення банківської безпеки україни в умовах розвитку інформаційної економіки : дис. … д-ра екон. наук / Національний інститут стратегічних досліджень, Київ, 2019. 531 с. URL: https://niss.gov.ua/sites/default/files/2020-02/gladkikh_disertacia.pdf.

2. Гладких Д. М. Ризики та можливості банківської системи України в умовах розвитку інформаційної економіки. *Аналітична записка. Серія «Економіка»* / *Національний інститут стратегічних досліджень*. 2019. № 4. 23 с. URL: https://niss.gov.ua/sites/default/files/2019-09/ANALIT%20GLADKYH%20ECONOMICS%20%23%204%202019_0.pdf.

3. Гудзь О. Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес*. 2019. № 3 (29). С. 4–12.

4. Європейська рада системного ризику («ESRB»). Звіт про системні кібератаки, лютий 2020. URL: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

5. Ільчук В. П., Парубець О. М., Сугоняко Д. О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. *Ефективна економіка*. 2018. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=6295.

6. Маргасова В. Г., Дубина М. В., Тунік М. В. Актуальні проблеми розвитку страхового ринку України. *Проблеми і перспективи економіки та управління.* 2015. № 2 (2). С. 219–228.

7. Нагайчук Н. Г., Третяк Н. М., Ткаленко О. О. Страхування в системі управління кіберризиками підприємства в умовах цифрової економіки. *Фінансовий простір*. 2019. № 1. С. 97-116. URL: http://nbuv.gov.ua/UJRN/Fin_pr_2019_1_8.

8. Річний звіт аудиторської компанії PwC «Страхування 2020 року і далі: отримання дивідендів від кібер-стійкості». URL: https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

9. Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава*. 2020. № 1. С. 23–26.

10. Сєдов Є. С. Деякі аспекти страхування кібер-ризиків. *Інноваційні напрямки розвитку страхового ринку України* : зб. матеріалів ІІІ Міжнар. наук.-практ. конф. (19–20 квіт. 2016 р., м. Київ). Київ : КТ «Забєліна-Фільковська Т. С. і компанія Київська нотна фабрика», 2016. С 288–291.

11. Щорічні витрати на кібербезпеку та кіберстрахування у всьому світі з 2015 по 2020 рік від Statista.com. URL: https://www.statista.com/statistics/387868/it-cyber-securiy-budget.

12. Arunabha Mukhopadhyay, Anirban Mahanti, Debashis Saha, Chakrabarti B. B., Podder A. Insurance for cyber-risk: A Utility Model. *Decision* (0304-0941). Jan-Jun 2005, Vol. 32. Issue 1, P. 153–169. URL: https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model.

13. Berzin P., Shyshkina O., Kuzmenko O., Yarovenko H. Innovations in the Risk Management of the Business Activity of Economic Agents. *Marketing and Management of Innovations*. 2018. Vol. 4. P. 221–233.

14. Böhme R., Schwartz G. Modeling cyber-insurance: Towards a unifying framework. *Ninth Annual Workshop on the Economics in Information Security (WEIS'10).* 2010.

15. Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *WP/18/143.* 2018. URL: https://www.researchgate.net/publication/326472318_Cyber_ Risk_for_the_ Financial_Sector_A_Framework_for_Quantitative_Assessment.

16. Laura A. Odell, J. Corbin Fauntleroy, Ryan R. Wagner. Cyber Insurance – Managing Cyber Risk. 2015. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a623798.pdf.

17. Marotta A., Martinelli F., Nanni S., Yautsiukhin A. A Survey on Cyber-Insurance. Bologna, Italy : Unipol Gruppo Finanziario S.p.A., 2015. 52 p.

18. Mirsanova O. The Bonus-Malus System as the policyholders' classification method in cyber-insurance. *Economics: Yesterday, Today and Tomorrow.* 2016. № 6. P. 10–23. URL: https://www.academia.edu/28843171/The_Bonus-Malus_System_as_the_policyholders_classification_method_in_cyber-insurance_Olga_Mirsanova.

19. Official Annual Cybercrime Report 2019. Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades / Ed. Steve Morgan. Herjavec Group. 12 p. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

20. Phishing Activity Trends Report – 4Q 2019. Anti-Phishing Working Group – Released February 24, 2020. URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf.

21. Romanosky S., Ablon L., Kuehn A., Jones T. Content Analysis of Cyber Insurance Policies: How do carriers price cyber risk? *Journal of Cybersecurity*. 2019. P. 1–19.

22. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Research, 2019. Accenture. URL: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

23. The Global Risks Report 2019: 14th Edition. World Economic Forum. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

24. U.S. Cyber Insurance Market Share and Performance (Premium Expansion Slows amid Favorable Performance in 2018). URL: https://www.fitchratings.com/research/insurance/cyber-insurance-growth-slows-market-remains-untested-14-05-2019.

25. Yıldırım İsmail. Cyber Risk Management in Banks: Cyber Risk İnsurance-Bankalarda Siber Risklerin Yönetimi: Siber Risk Sigortası. November 2018. URL: https://www.researchgate.net/publication/328811808_Cyber_Risk_Management_in_Banks_Cyber_Risk_Insurance-Bankalarda_Siber_Risklerin_Yonetimi_Siber_Risk_Sigortasi.

References

1. Hladkykh, D. M. (2019). *Zabezpechennia bankivskoi bezpeky ukrainy v umovakh rozvytku informatsiinoi ekonomiky [Ensuring banking security of Ukraine in terms of information economy]* (Candidate`s thesis). Natsionalnyi instytut stratehichnykh doslidzhen, Kyiv. Retrieved from https://niss.gov.ua/sites/default/files/2020-02/gladkikh_disertacia.pdf.

2. Hladkykh, D. M. (2019). Ryzyky ta mozhlyvosti bankivskoi systemy Ukrainy v umovakh rozvytku informatsiinoi ekonomiky [Risks and opportunities of the banking system of Ukraine in the terms of the information economy development]. *Analitychna zapyska. Seriia «Ekonomika» – Analytical note. Series "Economics",* 4. Retrieved from https://niss.gov.ua/sites/default/files/2019-09/ANALIT%20GLADKYH%20ECONOMICS%20%23%204%202019_0.pdf.

3. Hudz, O. Ye. (2019). Rozvytok strakhuvannia: novi instrumenty ta metody upravlinnia ryzykamy v tsyfrovii ekonomitsi [Development of insurance: new tools and methods of risk management in the digital economy]. *Ekonomika. Menedzhment. Biznes – Economy. Management. Business,* 3 (29), 4–12 [in Ukrainian].

4. Yevropeiska rada systemnoho ryzyku («ESRB»). Zvit pro systemni kiberataky [European Systemic Risk Board ("ESRB"). Systemic Cyber Attack Report]/ (February 2020). Retrieved from https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

5. Ilchuk, V. P., Parubets, O. M., Suhoniako, D. O. (2018). Innovatsiini pidkhody do rozvytku rynku kiberstrakhuvannia v Ukraini [Innovative approaches to the development of the cyber insurance market in Ukraine]. *Efektyvna ekonomika – Efficient economy,* 5. Retrieved from http://www.economy.nayka.com.ua/?op=1&z=6295.

6. Marhasova, V. H., Dubyna, M. V., Tunik, M. V. (2015). Aktualni problemy rozvytku strakhovoho rynku Ukrainy [Actual problems of the development of insurance market of Ukrainian]. *Problemy i perspektyvy ekonomiky ta upravlinnia – Problems and prospects of economics and management*, 2 (2), 219–228 [in Ukrainian].

7. Nahaichuk, N. H., Tretiak, N. M., Tkalenko, O. O. (2019). Strakhuvannia v systemi upravlinnia kiber-ryzykamy pidpryiemstva v umovakh tsyfrovoi ekonomiky [Insurance in cyber-risk management system of the enterprise in digital economy]. *Finansovyi prostir – Financial space,* 1, 97–116. Retrieved from http://nbuv.gov.ua/UJRN/Fin_pr_2019_1_8.

8. Richnyi zvit audytorskoi kompanii PwC «Strakhuvannia 2020 roku i dali: otrymannia dyvidendiv vid kiber-stiikosti» [Annual report of the audit company PwC "Insurance 2020 and beyond: receiving dividends from cyber resilience"]. Retrieved from https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

9. Seliverstova, L. S., Trukhan, D. A. (2020). Pidkhody do rozvytku kiberstrakhuvannia yak sehmentu hlobalnoho strakhovoho rynku [Approaches to the development of cyber insurance as a segment of the global insurance market]. *Ekonomika ta derzhava – Economy and state*, 1, 23–26 [in Ukrainian].

10. Siedov, Ye. S. (2016). Deiaki aspekty strakhuvannia kiber-ryzykiv [Some aspects of cyber risk insurance]. *Innovatsiini napriamky rozvytku strakhovoho rynku Ukrainy: zb. materialiv III Mizhnar. nauk.-prakt. konf. – Innovative directions of the insurance market developmeng of Ukraine: coll. materials III International. scientific-practical conf.* (April 19-20, 2016, Kyiv) (pp. 288–291). Kyiv: KT «Zabielina-Filkovska T. S. i kompaniia Kyivska notna fabryka» [in Ukrainian].

11. Shchorichni vytraty na kiberbezpeku ta kiberstrakhuvannia u vsomu sviti z 2015 po 2020 rik vid Statista.com [Annual spending on cybersecurity and cyber insurance worldwide from 2015 to 2020 from Statista.com]. Retrieved from https://www.statista.com/statistics/387868/it-cyber-securiy-budget.

12. Arunabha, Mukhopadhyay, Anirban, Mahanti, Debashis, Saha; Chakrabarti, B. B., Podder, A. (Jan-Jun 2005). Insurance for cyber-risk: A Utility Model. *Decision* (0304-0941), 32 (1), 153–169. Retrieved from https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model.

13. Berzin, P., Shyshkina, O., Kuzmenko, O., Yarovenko, H. (2018). Innovations in the Risk Management of the Business Activity of Economic Agents. *Marketing and Management of Innovations*, 4, 221–233.

14. Böhme, R., Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. *Ninth Annual Workshop on the Economics in Information Security (WEIS'10).*

15. Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *WP/18/143.* Retrieved from https://www.researchgate.net/publication/326472318_Cyber_Risk_for_the_Financial_Sector_A_Framework_for_Quantitative_Assessment.

16. Laura A. Odell, J. Corbin Fauntleroy, Ryan R. Wagner. (2015). *Cyber Insurance – Managing Cyber Risk.* Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a623798.pdf.

17. Marotta, A., Martinelli, F., Nanni, S., Yautsiukhin, A. (2015). *A Survey on Cyber-Insurance.* Bologna, Italy: Unipol Gruppo Finanziario S.p.A.

18. Mirsanova, O. (2016). The Bonus-Malus System as the policyholders' classification method in cyber-insurance. *Economics: Yesterday, Today and Tomorrow,* 6, 10–23. Retrieved from https://www.academia.edu/28843171/The_Bonus-Malus_System_as_the_policyholders_classification_method_in_cyber-insurance_Olga_Mirsanova.

19. Steve Morgan (Ed). (2019). Official Annual Cybercrime Report 2019. Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. Herjavec Group. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

20. Phishing Activity Trends Report – 4Q 2019. Anti-Phishing Working Group – Released (February 24, 2020). Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf.

21. Romanosky, S., Ablon, L., Kuehn, A., Jones, T. (2019). Content Analysis of Cyber Insurance Policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 1–19.

22. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Research (2019). Accenture. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

23. The Global Risks Report 2019: 14th Edition. World Economic Forum (2019). Retrieved from http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

24. U.S. Cyber Insurance Market Share and Performance (Premium Expansion Slows amid Favorable Performance in 2018) (2019). Retrieved from https://www.fitchratings.com/research/insurance/cyber-insurance-growth-slows-market-remains-untested-14-05-2019.

25. Yıldırım, İsmail. (November 2018). Cyber Risk Management in Banks: Cyber Risk İnsurance-Bankalarda Siber Risklerin Yönetimi: Siber Risk Sigortası. Retrieved from https://www.researchgate.net/publication/328811808_Cyber_Risk_Management_in_Banks_Cyber_Risk_Insurance-Bankalarda_Siber_Risklerin_Yonetimi_Siber_Risk_Sigortasi.

Дубина Максим Вікторович – доктор економічних наук, доцент, завідувач кафедри фінансів, банківської справи та страхування, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Дубина Максим Викторович – доктор экономических наук, доцент, заведующий кафедрой финансов, банковского дела и страхования, Черниговский национальный технологический университет (ул. Шевченко, 95, г. Чернигов, 14035, Украина).
Dubyna Maksym – Doctor of Economics, Associate Professor, Head of the Department of Finance, Banking and Insurance, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: maksim-32@ukr.net; mvdubyna@gmail.com
ORCID: http://orcid.org/0000-0002-5305-7815
ResearcherID: F-3291-2014
Scopus Author ID: 56912277800

Середюк Ірина Олександрівна – магістр, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Середюк Ирина Александровна – магистр, Черниговский национальный технологический университет (ул. Шевченко, 95, г. Чернигов, 14035, Украина).
Serediuk Iryna – master, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: i.seredyuk36@gmail.com
ORCID: http://orcid.org/0000-0002-6100-7164

Білоус Наталія Вікторівна – магістр, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Наталья Белоус Викторовна – магистр, Черниговский национальный технологический университет (ул. Шевченко, 95, г. Чернигов, 14035, Украина).
Bilous Natalia – master, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).