УДК 336.368

Н. В. Приказюк,
д. е. н., доцент, завідувач кафедри страхування, банківської справи та ризик-менеджменту,
Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0002-7813-8590
Л. С. Гуменюк,
магістр, спеціальність "Фінанси, банківська справа та страхування",
Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0002-2803-913X

DOI: 10.32702/2306-6814.2020.15—16.28

ПЕРЕДУМОВИ РОЗВИТКУ КІБЕР-СТРАХУВАННЯ

N. Prykaziuk,
Doctor of Economic Sciences, Associate Professor, Head of the Department of Insurance,
Banking and Risk Management, Taras Shevchenko National University of Kyiv
L. Gumenyuk,
Master of the Departament of Finance, banking and risk management,
Taras Shevchenko National University of Kyiv

PREREQUISITES FOR THE DEVELOPMENT OF CYBER INSURANCE

У статті виявлено, що вдосконалення інформаційних технологій впливає на зміну формату діяльності зловмисників, що пов'язано з використанням IT-інструментарію та Інтернет-мережі. Визначено етапи зародження та подальшого розвитку кібер-страхування в умовах третьої промислової революції. З'ясовано ключові події на кожному з етапів цифрової трансформації промисловості та економіки. Обгрунтовано основні передумови розвитку кібер-страхування на кожному з етапів. Розглянуто Hype Cycle для страхування з 2015 року, відповідно за яким виокремлено, що основними перспективними інструментами є BigData, Clouds, IoT, AI. Розроблено Hype Cycle для страхування з 2020 року, за яким визначені адаптивні моделі комунікації, віртуалізація робочих місць, персоніфікація рекламних пропозицій, синтезія даних — як перспективні напрями розвитку кібер-страхування.

The article examines the improvement of information technology affects the change in the format of attackers, which is associated with the use of IT tools and the Internet. The stages of origin and further development of cyber insurance in the conditions of the third industrial revolution are determined. The key events at each stage of the digital transformation of industry and economy are identified. The main prerequisites for the development of cyber insurance at each stage are substantiated. The Hype Cycle for insurance 2015 is considered, according to which it is highlighted that the main promising tools are BigData, Clouds, IoT, AI. Hype Cycle for insurance has been developed 2020, which defines adaptive communication models, virtualization of workplaces, personalization of advertising offers, data synthesis — as promising areas of cyber insurance.

Each stage of industrial development was marked by revolutionary events related to the improvement of existing traditional processes or even their actual replacement by breakthrough tools. The third industrial revolution, characterized by the transition from analog to digital technologies, led to the emergence of an innovative type of insurance activity — cyber insurance. Thus, the digital revolution is directly related to the stages of development of cyber insurance.

At the stage of development of digital technologies, the precondition for the emergence of cyber insurance was the formation and improvement of information systems, which could be accessed by attackers, or which could cease to function properly.

During the mass release of digital technologies, further improvement of information systems and the development of affordable personal computers with clear software led to a wave of fraud with personal data of users, and therefore there was a direct need for cyber insurance as a tool to protect sensitive data.

Another important prerequisite for the development was the launch and spread of the Internet, because, on the one hand, it enabled the connection of many devices in real time, and on the other hand, became a tool for attackers to access user data and organizations. This stage is marked by the actual creation of cyber-insurance, as in this period in the insurance policy were introduced definitions of information risks.

The transition to a digital business model is associated with the further development and improvement of cyber-insurance tools. It is the global proliferation of personal computers, mobile phones, ATMs, the increase in the functionality of the Internet and browsers that has led to the development of the shadow IT segment, which aims to steal, damage and hack software, mechanisms and databases.

Ключові слова: кібер-страхування, кібер-ризик, кібер-атака, кібер-захист, підприємство, інформація, цифрова трансформація.

Key words: cyber insurance, cyber risk, cyber attack, cyber protection, enterprise, information, digitalization.

ПОСТАНОВКА ПРОБЛЕМИ

В умовах третьої промислової революції, яка характеризується автоматизацією виробництва, переходом на автономний формат праці та цифрову трансформацію усіх сфер діяльності, важливим аспектом стає кібербезпека. В свою чергу кібер-страхування є дієвим інструментом, який попереджує настання кібер-інцидентів, а також мінімізує втрати у разі їх настання.

На сьогодні питання становлення та розвитку кібер-страхування є одним із ключових, оскільки повне розуміння передумов зародження зазначеного виду страхування дозволить визначити основні драйвери, які сприяють розвитку інноваційних видів діяльності.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблематику створення та поширення кібер-страхування вивчали такі вітчизняні науковці: Н.М. Внукова, О.О. Гаманкова, Ю.П. Гришан, О.М. Залєтов, А.Д. Заруба, Р.В. Пікус, а також зарубіжні вчені: Дж. Арчі, К. Сарда, Дж. Фінкл. На сьогодні недостатньо розкритими є передумови виникнення кібер-страхування в рамках цифрової трансформації, оскільки існує потреба у окресленні ключових драйверів розвитку кібер-страхування задля його подальшого вдосконалення та закріпленні на страховому світовому ринку.

МЕТА ДОСЛІДЖЕННЯ

Метою роботи є виявлення основних передумов становлення та подальшого розвитку кібер-страхування як важливого механізму захисту підприємств в умовах цифрової трансформації.

Для досягнення поставленої мети в роботі окреслено і вирішено такі завдання:

— визначити етапи становлення кібер-страхування;

— охарактеризувати основні передумови виникнення кібер-страхування на кожному етапі;

— з'ясувати ключові загальні причини розвитку кібер-страхування;

— визначити Hype Cycle для страхування з 2015 року;

— розробити Hype Cycle для страхування з 2020 року.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У 21 ст., в умовах миттєвої доступності будь-якого девайсу до Інтернет-мережі, особливої важливості набуває питання цифрової безпеки. Оскільки цифровізація має хвилеподібний характер, тому після винайдення нових технологій, які полегшують та вдосконалюють існуючі системи, виникають злочинні інструменти, які знищують та викрадають інформацію з вказаних систем. Зрозуміло, що на різних етапах розвитку технологій, важливість деяких даних оцінювалась по-різному, але завжди на злочинному ринку був попит на відповідний товар. Оскільки не існує жодної довершеної системи, тому ймовірність кібер-інцидентів на сьогодні доволі висока. Саме тому кібер-страхування виступає ефективним інструментом мінімізації збитків від настання страхових подій.

Розвиток кібер-страхування тісно пов'язаний з третьою промисловою революцією (цифровою трансформацією промисловості та економіки), оскільки саме з поступовим введенням IT-інструментарію в побутове використання виникли можливості цифрового шахрайства. Таким чином, вважаємо за доцільне виокремити 5 основних етапів розвитку кібер-страхування у відповідності до періодів цифрової революції (табл. 1).

З початком розвитку інноваційних технологій поступово формувалась потреба у цифровій безпеці. У випадку її порушення, "подушкою" безпеки для організацій стало кібер-страхування.

У період зародження перших цифрових технологій у 1947—1969 роках перед власниками організацій не виникала проблема у захисті інформації у сучасному розумінні, оскільки більшість конфіденційних даних була засекречена та надавалась лише за наявності спеціального доступу, або ж передавалась через листи чи телеграми, тому зрозуміти факт викрадення даних було важ-

Таблиця 1. Етапи становлення кібер-страхування

Період	Назва	Ключові події
1947-1969 рр.	Зародження цифрових технологій	– Винахід цифрового резистора, який вдосконалив роботу цифрових комп'ютерів; – реалізація МОР-мікросхем, що призвело до виникнення першого мікропроцесора; – розвиток технології MOS, яка дозволила створити датчики зображень, що стали основою цифрових камер
1969-1989 рр.	Масовий випуск цифрових технологій	– Створення та поширення Інтернет-мережі на побутовому рівні; – розробка доступних ПК, ігрових консолей та аркадних відео-ігор; – встановлення банкоматів, промислових роботів, створення дошок оголошення в Інтернеті; – додавання комп'ютерної графіки у кіно та іграх, електронна музика; – випуск першого мобільного телефону, цифрової камери
1989-2005 рр.	Фактичне створення кібер-страхування	– Запуск всесвітньої мережі, яка об'єднала ПК; – стрімкий розвиток Інтернет-інструментів; – розгалуження можливостей мобільних телефонів, ПК; – масове використання текстовими повідомленнями, як альтернативним каналом зв'язку
2005-2015 рр.	Розширення та вдосконалення кібер-страхового інструментарію	– Більше 1 млрд користувачів Інтернет-мережі; – розповсюдження цифрових технологій; – перехід від офсетного до цифрового друку; – масовий продаж смартфонів
Після 2015 р.	Реалізація нормативно-правового забезпечення кібер-страхування	– Реалізація IoT, 3D Print; – розвиток BigData, Cloud технологій; – перехід на цифрову модель ведення бізнесу

Джерело: Складено авторами на основі [1—4; 8].

че. Але саме у цьому періоді був винайдений цифровий резистор, що став основою для збору цифрового комп'ютера; МОР-мікросхема, на якій працював перший мікропроцесор; технологія MOS, яка створила прототип сучасної цифрової камери. Отже, саме середина 20 ст. стала початком розвитку технологій, що спричинили третю промислову революцію. На даному етапі перед організаціями була задача максимізації ефективності та якості виробництва, що стало можливим після введення даних технологій у масове виробництво.

На цьому етапі передумовами виникнення кібер-страхування стали:

— створення інструментів, які мали доступ до особливої інформації про організації, які їх використовують;

— поширення технологій, експертами з розвитку/вдосконалення яких були спеціалісти іноді єдині у своїй справі;

— переведення більшої частині інформації на цифрові носії, реалізація баз даних, які надавали швидкий доступ до великих об'ємів інформації.

Після підготовчого етапу протягом 1969 — 1989 років було запущено понад 50 напрямів цифрового вдосконалення. Одним із найбільших досягнень цього періоду стало створення та поширення Інтернет-мережі, щоправда з обмеженим функціоналом. Також, завдячуючи здобуткам попереднього етапу, вдалося зібрати та запустити у масове виробництво доступних варіантів персональних комп'ютерів, ігрових консолей з простими акрадними відео-іграми. Через деякий час були встановлені мобільні роботизовані точки: банкомати, термінали, інформаційні табло та інше. Також радикальні зміни торкнулись сфери кіно — почалось використання комп'ютерної графіки задля створення візуальних та аудіо-ефектів у фільмах; сфери музики — оскільки звукові ефекти створювались електронними генераторами.

Після цього у 1973 році був випущений перший прообраз мобільного телефону Motorola DynaTAC, з якого ж був здійснений перший мобільний дзвінок.

Також варто зазначити, що на цьому етапі були проведенні перші тестування по цілісності систем та їх безпеці, а тому були реалізовано ряд захисних розробок для них.

Такі проривні трансформації додали ще кілька причин розвитку кібер-страхування:

— масове поширення персональних комп'ютерів, ігрових консолей та мобільних телефонів;

— встановлення банкоматів та терміналів, які зчитували конфіденційні дані з особистих кратк власників;

— створення дошок-оголошень в Інтернеті, які стали платформою для збору шахраями особистих даних користувачів.

З 1989 по 2005 рік активно вдосконалювались ПК, мобільні телефони, цифрові камери та інше, при цьому створюючи закриту систему обміну інформацією — передача відбувалась за допомогою мережі Інтернет, тому даний канал передачі даних став об'єктом для зловмисників. Частими стали випадки злому пошти, особистих кабінетів, або ж публічного оприлюднення конфіденційних даних підприємств та навіть урядових організацій. Виникло поняття Інтернет-вірусу, який міг пошкоджувати системні файли комп'ютерів та телефонів.

Органічним наслідком стало створення антивірусних систем, які все ж залишали ймовірність поломки системи або витоку інформації. Для більшості організацій створення окремого фонду на випадок кібер-інцидентів було доволі обтяжливим, оскільки іноді втрати

Таблиця 2. Матриця відповідності етапів становлення кібер-страхування періодам цифрової трансформації промисловості

Передумови	Зародження цифрових технологій	Масовий випуск цифрових технологій	Фактичне створення кібер-страхування	Розширення та вдосконалення кібер-страхового інструментарію	Реалізація нормативно-правового забезпечення кібер-страхування
Створення/вдосконалення інформаційних технологій та систем	+	+	+	+	+
Винахід доступних ПК та інших цифрових пристроїв	-	+	+	+	+
Популяризація використання Інтернет-мережі	-	+	+	+	+
Перехід на цифрову модель ведення бізнесу	-	-	+	+	+
Збільшення кількості ПЗ, додатків; об'ємів даних	-	-	-	+	+

Джерело: складено авторами на основі [1—4; 8].

могли сягати мільйонів доларів. Тому під час страхування компанії окреслювали даний вид ризику та включали його як окреме джерело збитків. Відповідно, у цей період було вперше виділені інформаційні та цифрові ризики, які є основою кібер-страхування.

Даний етап вважаємо початком існування кібер-страхування з наступними причинами його подальшого вдосконалення:

— об'єднання усіх пристроїв через Інтернет-мережу;

— збільшення кількості каналів передачі даних, які не були повністю захищеними;

— низький рівень обізнаності населення у IT-сфері;

— непрозорість встановлення програмного забезпечення на ПК та мобільні телефони.

Після 2005 року у світі нараховувалось більше 1 млрд користувачів, які щоденно користувались Інтернет-мережею. Відповідно, збільшувались і доступні інструменти: соціальні мережі, сайти знайомств, онлайн телефонія, платформи продажу, ігри, платіжні системи та інше. Оскільки обсяги доступної інформації зростали, то збільшувались об'єкти для атак зловмисників. Інтернет-грамотність населення та організацій була на низькому рівні, системи могли бути скомпрометовані через випадкові дії внутрішніх користувачів ПК.

З 2005 року почався масовий продаж смартфонів, які гіпотетично мали стати аналогом комп'ютера у зменшеному вигляді. З плином часу, розробникам вдалось перенести багато процесів, які раніше були доступні тільки ПК, на смартфон. Даний період співпадає з початком масових зломів особистих поштових кошиків, тому можемо зробити висновок, що спрощення доступу до листування надало привілеї зловмисникам у використанні зашифрованої інформації.

Тому передумовами подальшого вдосконалення кібер-страхування вважаємо:

— глибока пенетрація Інтернет-мережі (51% домогосподарств та організацій);

— розповсюдження смартфонів як альтернатива мобільним телефонам та комп'ютерам;

— реалізація великої кількості не сертифікованих мобільних додатків та програмного забезпечення;

— збільшення частки електронних платежів (з введенням персональних даних).

Протягом останніх 5 років цифрова трансформація проявляється через перехід на автоматизовані системи, які можуть самостійно навчатись. Так, популярності набувають нейромережі, штучний інтелект, хмарні обчислювальні системи та сховища даних, технології BigData та IoT.

Такі системи є більш безпечними та захищеними, оскільки зменшують можливість людського втручання. Також робота з великими масивами інформації стало основою переходу до хмарних сховищ збереження даних, доступ до яких часто є закритим навіть для IT-спеціалістів. Але водночас ймовірність зупинки роботи цих систем все ще є актуальною, тому важливість мінімізації наслідків після інциденту все ще важлива.

Кібер-страхування на даному етапі виступає не просто інструментом по мінімізації наслідків, а й ефективним механізмом попередження їх настання, оскільки забезпечує співпрацю зі спеціалізованими організаціями-експертами з захисту систем та конфіденційної інформації (партнерські програми) та попередній моніторинг стану клієнта.

Також на цьому етапі було розпочато роботу над нормативно-правовим забезпеченням, яке регулює відносини у сфері кібер-страхування.

На сьогодні є необхідність у розвитку кібер-страхування, що зумовлена такими факторами:

— наявність великих обсягів інформації, яка щоденно генерується будь-яким обчислювальним пристроєм або системою;

— швидкий розвиток BigData та Cloud технологій, які можуть замінити сучасні бізнес-процеси;

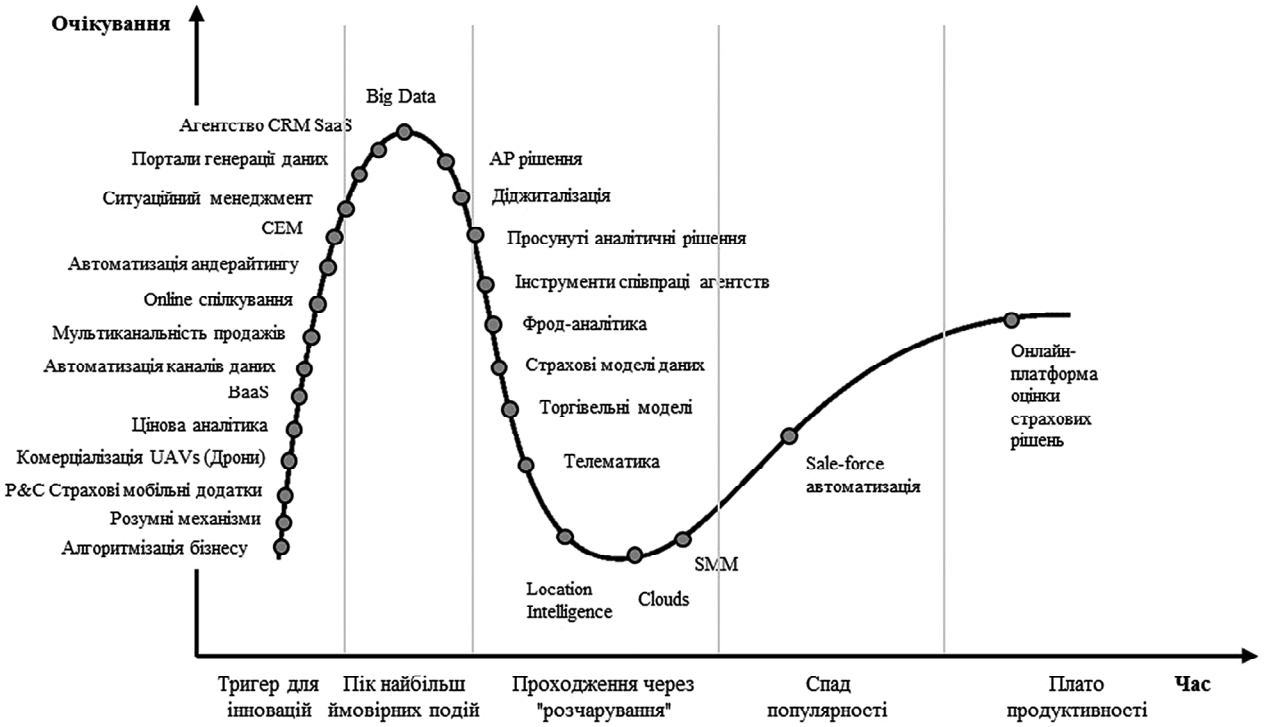

Рис. 1. Gartner Hype Cycle для страхування 2015 р.

Джерело: складено авторами на основі [11].

— відсутність єдиного підходу до визначення учасників та об'єктів кібер-страхування.

Отже, на кожний період цифрової трансформації припадали різні винаходи та вдосконалення, цінність яких відрізнялась на кожному з етапів. Тому, узагальнюючи, можна визначити такі передумови виникнення кібер-страхування:

— створення/вдосконалення інформаційних технологій та систем;

— винахід доступних ПК та інших цифрових пристроїв;

— популяризація використання Інтернет-мережі;

— перехід на цифрову модель ведення бізнесу;

— збільшення кількості ПЗ, додатків; обсягів даних.

Важливо розуміти, які причини стали основними у становленні кібер-страхування, оскільки окреслення драйверів розвитку є основою подальшої стратегії вдосконалення (табл. 2).

Отже, виходячи з отриманих результатів, бачимо, що створення та вдосконалення інформаційних технологій та систем провокує розвиток і шахрайських інструментів, що в свою чергу зобов'язує компанії та домогосподарства створювати безпечні умови існування з використання кібер-страхування. До того ж постійне вдосконалення механізмів спостерігалось з самого початку цифрової трансформації, а тому потреба у інформаційній та цифровій захищеності була сформована ще у 20 ст.

Наступною за актуальністю передумовою є популяризація Інтернет-мережі та наявність доступних персональних комп'ютерів та інших девайсів на ринку. Широкий вибір різнозадачних інструментів став основою низької освіченості користувачів, які стали об'єктами атак зловмисників. На сьогодні Інтернет-мережа стала платформою, які замінює більшість традиційних процесів в усіх сферах економіки. Так, за даними eMarketer, до кінця 2020 року доля роздрібних продажів, реалізованих через Інтернет, складе 14,6%, що вдвічі більше, ніж в 2015 році. Частка розрахунків, які здійснюються через мобільні пристрої у 2019 році склала 30%, при тому, що 68% кібер-інцидентів, пов'язаних з компрометацією банківських карт, здійснились через смартфони [10]. Тому стрімке розповсюдження кібер-страхування пояснюється низьким рівнем обізнаності основ функціонування електронних платіжних систем та великою кількістю їх шахрайських дублікатів.

З розвитком інноваційних технологій змінився традиційний шлях ведення бізнесу, що виражається через запровадження автоматизованого виробництва з оптимізацією навантаження на них, а тому зменшення можливості людської похибки при доступі до них. Зворотною стороною цього є генерування та зберігання великих обсягів даних, які в разі викрадення, можуть бути використані проти компаній (вплив на репутацію, або прямий доступ до внутрішніх систем).

Підтвердженням наших висновків є запропонована компанією Gartner діаграма Hype Cycle, яка відображає цикли очікування, реалізації та використання певних технологій. У 2016 році компанією була розроблена аналогічна візуалізація, яка відображає стан доступних та майбутніх технологій для страхування (рис. 1).

За аналогією віднайдемо технології та інструменти, які будуть актуальні для страхування, починаючи з 2020 року. Для цього визначимо тригери для інновацій у 2020 році (з врахуванням пандемії), а також пікові події, які стануть актуальними для страхування у найближчих 5 років. Відповідно, окреслимо інструментарій, який стане менш популярним та збитковим у використанні (рис. 2).

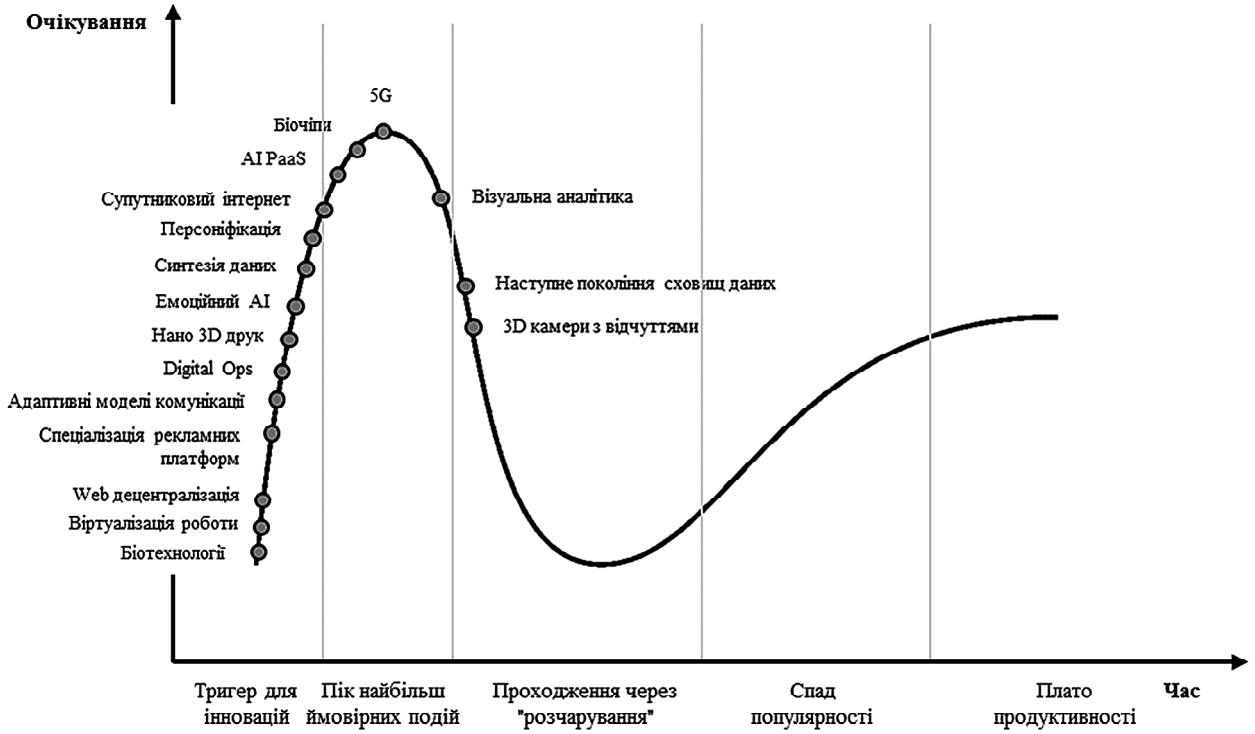

Рис. 2. Gartner Hype Cycle для страхування 2020 р.

Джерело: складено авторами на основі [6; 9].

Таким чином, у майбутньому ключовими технологіями, які стануть драйверами вдосконалення та розвитку кібер-страхування ми вважаємо віртуалізацію робочих місць, децентралізацію автономної роботи організації, запуск 5G, вдосконалення і розширення можливостей 3D друку, персоніфікацію та глибинну аналітику.

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ У ЦЬОМУ НАПРЯМІ

Кожний етап розвитку промисловості відзначався революційними подіями, що пов'язані з вдосконалення існуючих традиційних процесів або навіть їх фактичним заміщенням проривними інструментами. Третя промислова революція, яка характеризується переходом з аналогових технологій на цифрові, зумовила виникнення інноваційного виду страхової діяльності — кібер-страхування. Таким чином, цифрова революція напряму пов'язана з етапами розвитку кібер-страхування.

На етапі розвитку цифрових технологій передумовою виникнення кібер-страхування стало формування та вдосконалення інформаційних систем, до яких могли отримати доступ зловмисники, або які могли припинити коректне функціонування.

У період масового випуску цифрових технологій, подальше вдосконалення інформаційних систем та розробка доступних персональних комп'ютерів з зрозумілим програмним забезпеченням зумовила хвилю махінацій з особистими даними користувачів, а тому і виникла пряма необхідність у кібер-страхуванні, як інструменті захисту конфіденційних даних.

Ще однією важливою передумовою розвитку став запуск та поширення Інтернет-мережі, оскільки, з одного боку, це надало можливість з'єднання безлічі девайсів у режимі реального часу, а з іншого — стало інструментом зловмисників, задля доступу до даних користувачів та організацій. Саме цей етап і відзначається фактичним створенням кібер-страхування, бо в цей період у поліси страхування були внесені означення інформаційних ризиків.

З переходом на цифрову модель ведення бізнесу пов'язують подальший розвиток та вдосконаленням кібер-страхового інструментарію. Саме глобальне розповсюдження персональних комп'ютерів, мобільних телефонів, банкоматів, збільшення функціональну Інтернет-мережі та браузерів зумовило розвиток тіньового IT-сегменту, завданням якого є викрадення, псування та злом програмного забезпечення, механізмів та баз даних.

Поступове розширення промислових можливостей стало органічним поштовхом розвитку інших сфер діяльності, в тому числі і злочинної. Саме тому, на противагу зловмисникам, було виокремлено послуги страховиків, які стосуються захисту конфіденційної інформації, цілісності баз даних, збереженості виробничих потужностей — кібер-страхування.

Література:

1. Digital Medicine: Implications for Healthcare Leadershttps [Електронний ресурс]. — Режим доступу: //archive.org/details/digitalmedicinei0000gold (Дата звернення: 18.08.2020).

2. Art & Computers: an exploratory investigation on the digital transformation of art [Електронний ресурс]. — Режим доступу: http://www.doctorhugo.org/synaesthesia/e-tsyn.htm (Дата звернення: 18.08.2020).

3. Digital Europe: Realizing the continent's potential [Електронний ресурс]. — Режим доступу: https://www.mckinsey.com/business-functions/mckinsey-

digital/our-insights/digital-europe-realizing-the-continents-potential (Дата звернення: 18.08.2020).

4. Leadership in the Digital Age — a study on the effects of digitalization on top management leadership [Електронний ресурс]. — Режим доступу: https://su.diva-portal.org/smash/get/diva2:971518/FULLTEXT02.pdf (Дата звернення: 18.08.2020).

5. How Digital Disruption Impacts Manufacturing Industry [Електронний ресурс]. — Режим доступу: https://hexaware.com/blogs/how-digital-disruption-impacts-manufacturing-industry/ (Дата звернення: 18.08.2020).

6. The Impact of Digitalization on Finnish Organizations [Електронний ресурс]. — Режим доступу: https://aaltodoc.aalto.fi/bitstream/handle/123456789/16540/isbn9789526062433.pdf?sequence=1&isAllowed=y (Дата звернення: 18.08.2020).

7. The case for digital reinvention [Електронний ресурс]. — Режим доступу: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-case-for-digital-reinvention (Дата звернення: 18.08.2020).

8. Remarks by Director Iancu at the 2019 International Intellectual Property Conference [Електронний ресурс]. — Режим доступу: https://www.uspto.gov/about-us/news-updates/remarks-director-iancu-2019-international-intellectual-property-conference (Дата звернення: 18.08.2020).

9. IDC says get on board with the DX economy or be left behind [Електронний ресурс]. — Режим доступу: https://searcherp.techtarget.com/news/450414723/IDC-says-get-on-board-with-the-DX-economy-or-be-left-behind (Дата звернення: 18.08.2020).

10. Insurance IT/Tech Expenses, UK [Електронний ресурс]. — Режим доступу: https://www.emarketer.com/forecasts/5f3ae4d277c0d402a876a40a/5f3ae3ae77c0d402a876a402 (Дата звернення: 18.08.2020).

11. Gartner Agency [Електронний ресурс]. — Режим доступу: https://www.gartner.com/en (Дата звернення: 18.08.2020).

References:

1. Goldsmith, J. Ch. (2003), "Digital Medicine: Implications for Healthcare Leadershttps", [Online], available at: //archive.org/details/digitalmedicinei0000gold (Accessed 18 Aug 2020).

2. Heyrman, H. (1997), "Art & Computers: an exploratory investigation on the digital transformation of art", [Online], available at: http://www.doctorhugo.org/synaesthesia/e-tsyn.htm (Accessed 18 Aug 2020).

3. Bughin, J. Hazan, E. Labaye, E. Manyika, J. Dahlstrom, P. Ramaswamy, S. and Cochin de Billy, C. (2016), "Digital Europe: Realizing the continent's potential", [Online], available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-europe-realizing-the-continents-potential (Accessed 18 Aug 2020).

4. Stockholm Business School (2016), "Leadership in the Digital Age — a study on the effects of digitalization on top management leadership", [Online], available at: https://su.diva-portal.org/smash/get/diva2:971518/FULLTEXT02.pdf (Accessed 18 Aug 2020).

5. Hexaware Technologies Limited (2018), "How Digital Disruption Impacts Manufacturing Industry", [Online], available at: https://hexaware.com/blogs/how-digital-disruption-impacts-manufacturing-industry/ (Accessed 18 Aug 2020).

6. Collin, J. Hiekkanen, K. Korhonen, J. J. Halen, M. Itala, T. and Helenius, M. (2015), "The Impact of Digitalization on Finnish Organizations", [Online], available at: https://aaltodoc.aalto.fi/bitstream/handle/123456789/16540/isbn9789526062433.pdf?sequence=-1&isAllowed=y (Accessed 18 Aug 2020).

7. Bughin, J. LaBerge, L. and Mellbye A. (2017), "The case for digital reinvention", [Online], available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-case-for-digital-reinvention (Accessed 18 Aug 2020).

8. USPTO (2019), "Remarks by Director Iancu at the 2019 International Intellectual Property Conference", [Online], available at: https://www.uspto.gov/about-us/news-updates/remarks-director-iancu-2019-international-intellectual-property-conference (Accessed 18 Aug 2020).

9. O'Donnell, J. (2017), "IDC says get on board with the DX economy or be left behind", [Online], available at: https://searcherp.techtarget.com/news/450414723/IDC-says-get-on-board-with-the-DX-economy-or-be-left-behind (Accessed 18 Aug 2020).

10. eMarketer (2020), "Insurance IT/Tech Expenses", UK, [Online], available at: https://www.emarketer.com/forecasts/5f3ae4d277c0d402a876a40a/5f3ae3ae77c0d402a876a402 (Accessed 18 Aug 2020).

11. Gartner Agency (2020), [Online], available at: https://www.gartner.com/en (Accessed 18 Aug 2020).

Стаття надійшла до редакції 20. 08. 2020 р.