УДК 004.056:338.47
DOI: https://doi.org/10.32782/2415-8801/2020-1.6

Дем'янчук М.А.
кандидат економічних наук,
доцент кафедри фінансів, банківської справи та страхування,
Одеський національний університет імені І.І. Мечникова

ПРОЦЕСНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ЗАСОБІВ ЗАХИСТУ АКТИВІВ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА ВНАСЛІДОК ВИНИКНЕННЯ КІБЕРІНЦИДЕНТІВ

У роботі обґрунтовано застосування процесного підходу до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів, який засновано на дослідженні технологій, що використовуються таким підприємством. Визначено його вразливі елементи під час діджиталізації із виявленням загроз та можливих наслідків, які впливають на активи, а також представлено засоби управління/особливості захисту. З метою розроблення та впровадження керівництвом підприємства необхідних дій із мінімізації кіберризиків залежно від каналів джерел кіберзагроз та видів ризику сформовано матрицю визначення ступеню кіберризику телекомунікаційного підприємства: низького, помірного, значного, високого. Запропоновано матрицю оцінки збитків телекомунікаційного підприємства від кіберінциденту, яка дає змогу, з одного боку, розподілити збиток на фінансовий та майновий, а з іншого – виокремити прямі витрати та витрати відповідальності.

Ключові слова: *телекомунікаційне підприємство, діджиталізація, інформаційна безпека, кібербезпека, кіберзагрози, кіберризик, кіберінцидент, кіберстійкість.*

ПРОЦЕССНЫЙ ПОДХОД К ОПРЕДЕЛЕНИЮ СРЕДСТВ ЗАЩИТЫ АКТИВОВ ТЕЛЕКОММУНИКАЦИОННОГО ПРЕДПРИЯТИЯ ВСЛЕДСТВИЕ ВОЗНИКНОВЕНИЯ КИБЕРИНЦИДЕНТОВ

Демянчук М.А.

В работе обосновано применение процессного подхода к определению средств защиты активов телекоммуникационного предприятия вследствие возникновения киберинцидентов, основанного на исследовании технологий, используемых таким предприятием. Определено его уязвимые элементы при диджитализации с выявлением угроз и возможных последствий, влияющих на активы, а также представлены средства управления/особенности защиты. С целью разработки и внедрения руководством предприятия необходимых действий по минимиза-

ции киберрисков в зависимости от каналов источников киберугроз и видов риска сформирована матрица определения степени киберриска телекоммуникационного предприятия: низкого, умеренного, значительного, высокого. Предложена матрица оценки ущерба телекоммуникационным предприятием от киберинцидента, которая позволяет, с одной стороны, распределить ущерб на финансовый и имущественный, а с другой – выделить прямые расходы и расходы ответственности.

Ключевые слова: *телекоммуникационное предприятие, диджитализация, информационная безопасность, кибербезопасность, киберугрозы, киберриск, киберинцидент, киберустойчивость.*

PROCESS APPROACH OF DETERMINING MEANS OF PROTECTION OF ASSETS OF A TELECOMMUNICATION ENTERPRISE DUE TO THE EMERGENCE OF CYBERINCIDENTS

Demianchuk Maryna

The digital economy is in an active phase of development, the main element of which is digital technology, which undoubtedly provides advantages and creates threats of new forms and types at different levels: from individuals, enterprises of various fields of economic activity and ending with national and world economies. The automation system of technological processes of critical enterprises, which primarily include telecommunications enterprises, is implemented as a digital control system distributed by functions and means and is represented by a combination of hardware and software that provide for the collection, accumulation, processing, provision and transmission of information. Therefore, an important question arises of the need to protect such critical objects as telecommunication enterprises from cyber attacks, especially in the process of transition from the classical paradigm of cybersecurity to the paradigm of cyber resistance. The methodological and information base was formed by the scientific works of domestic and foreign scientists on the issues presented, legislative and regulatory acts, analytical and statistical data. The aim of the work is to justify the application of the process approach in determining the means of protecting the assets of a telecommunication enterprise due to the occurrence of cyber incidents. Based on the analysis, systematization and generalization of modern definitions of the terms of economic, financial and information security, cybersecurity of enterprises, the concepts of cybersecurity of a telecommunication enterprise are identified, which should be understood as a set of measures to protect networks, applications, devices from threats and influences of an internal and external nature with the aim of confidentiality and integrity of enterprise data to ensure correct operation. A risk analysis was carried out for enterprises of different sizes and it was determined that the main risks are incidents in cyberspace and business interruptions (including a supply chain rupture). A process approach to determining the means of protection of the assets of a telecommunication enterprise due to the emergence of cyber incidents is presented, based on the study of the technologies used by such an enterprise, the identification of its vulnerable elements during digitalization with identification of threats and possible consequences affecting the assets, and management tools / protection features are presented. In order to develop and implement the necessary management actions by the enterprise management to minimize cyber risks, depending on the sources of cyber threats and types of risk, a matrix has been formed to determine the cyber risk of the telecommunications enterprise: low, moderate, significant, high. A matrix is proposed for assessing the damage of a telecommunication enterprise from cyber incident divided by financial into property, which allows, on the one hand, to allocate damage to financial and property, and, on the other, to distinguish direct expenses and liability expenses.

Keywords: *telecommunication enterprise, digitalization, information security, cybersecurity, cyber threats, cyber risk, cyber incident, cyber resistance.*

Постановка проблеми. Глобальний тренд цифрової світової економіки знаходиться в активній фазі свого розвитку. В Україні основними документами, що визначають необхідність формування та розвитку цифрової економіки і суспільства, є [1] та [2]. Цифровізація різних сфер економічної діяльності є головним елементом цифрової економіки у цілому, а цифрові технології є основою продуктових та виробничих стратегій. Використання новітніх технологій у сфері економіки дає змогу ефективніше використовувати знання класичної економіки для вирішення економічних проблем світу (кризових явищ, інфляції, збиткової економічної політики в деяких галузях), циклічних проблем. Однак інтеграція цифрових технологій відбувається не тільки у виробничу діяльність підприємств, а й у всі супутні, що робить підприємство відкритим в інформаційному просторі, і можливим стають і поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, здійснення незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Усе це зумовило створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [3].

Сучасна система автоматизації технологічних процесів критично важливих об'єктів, до яких належать передусім телекомунікаційні підприємства, реалізована як розподілена за функціями та засобами цифрова система управління. Вона представлена сукупністю апаратних та програмних засобів, які забезпечують збір, накопичення, обробку, надання та передачу інформації. Тому постає нагальне питання необхідності захисту таких критично важливих об'єктів, як телекомунікаційні підприємства, від кібернетичних атак, особливо у процесі переходу від класичної парадигми кібербезпеки до парадигми кіберсталості.

Аналіз останніх досліджень і публікацій. Різні проблематичні питання інформаційної та кібербезпеки підприємства: визначення апаратних загроз компонент шкідливого апаратного забезпечення, аналіз тлумачень та визначення понять, дослідження цифрової економіки, хактивізму та кібербезпеки тощо досліджують зарубіжні та вітчизняні вчені, серед яких слід відзначити Дж. Андрес, А.А. Артамонову, О.А. Бара-

нова, С. Бейделмана, Ю.В. Бородакія, С.В. Бреннера і М.Д. Гудмана, В.В. Буряка, П. Вуллей, А.Ю. Добродеева і І.В. Бутусова, О.Д. Довгань, Р.Л. Кіссель, С. Патела, В.П. Прохоренко, О.В. Сергієнков, А. Устенко, Ю. Черданцева та ін. Також слід відзначити існуючу серію міжнародних стандартів ISO/IEC 27000 з інформаційної безпеки, міжнародний стандарт ISO/IEC 18044 TR 18044:2004 з інформаційних технологій, фінансових послуг та рекомендацій стосовно інформаційної безпеки, стандарт NERC CIP, метою якого є гарантування захищеності автоматизованих систем та комунікаційних мереж від атак тощо. Приймаючи до уваги існуючи вагомі напрацювання теоретичного та прикладного характеру із досліджуваної проблематики у сучасних умовах проникнення цифровізації майже в усі сфери діяльності підприємств, зокрема телекомунікаційних, необхідним є розробленнй упровадження ефективних та дієвих засобів інформаційної безпеки.

Постановка завдання. Метою роботи є обґрунтування застосування процесного підходу до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів.

Виклад основного матеріалу дослідження. Цифрова економіка продовжує розширюватися по всьому світу, що в результаті стимулює все більшу кількість підприємств досліджувати нові сфері у своєму цифровому розвитку. Досягнення в галузі технологій, особливо у сфері аналітики і штучного інтелекту, сьогодні стають найбільш ефективними інструментами для бізнесу, оскільки цифрові системи є джерелом життєвої сили підприємства. Відбувається трансформація соціальних відносин, роботи підприємств та діяльності урядових органів – трансформація, яка засновує свій потенціал на технологіях, даних і штучному інтелекті, що збирають, фільтрують, класифікують і зіставляють величезні обсяги даних для того, щоб вчитися на них і робити прогнози. Цифрова трансформація впливає на повсякденне життя і роботу підприємств в таких масштабах, що нині вона стала джерелом його добробуту й інструментом забезпечення конкурентоспроможності. Цифрова трансформація, яка відбувається практично у всіх сферах життя, має особливе значення під час розгляду еволюції підприємств, організацій та державних структур як взаємопов'язаних пристроїв.

Сьогодні спостерігається різке зростання інцидентів у сфері інформаційної безпеки, які мають широке поширення і набувають загрозливого характеру. Багато з подібних атак стосуються широкого кола приватних, корпоративних, а також державних інтересів. Тобто стрімкий розвиток цифрової економіки супроводжується кіберзагрозами і кібер-ризиками для підприємств у вигляді шкідливих програм, ескалації організованої кіберзлочинності, порушення персональних даних та інформації, а також розширеної постійної загрози з боку Інтернету речей (IOT), мобільних і хмарних технологій. Усе це говорить про необхідність захисту підприємств в інформаційному просторі, проте не тільки у сфері кібертехнологій, пов'язаної з витоком або пошкодженням даних, а й фінансового захисту підприємства.

Існує безліч видів небезпек і загроз у середовищі функціонування телекомунікаційного підприємства, які зумовлюють безліч видів безпеки. В умовах цифрової економіки, що швидко розвивається, на перший план виходять поняття інформаційної та кібербезпеки. Під інформаційною безпекою Дж. Андрес розуміє практику запобігання несанкціонованому доступу, використанню, розкриттю, спотворенню, зміні, дослідженню, записам або знищенню інформації; збалансований захист конфіденційності, цілісності та доступності даних з урахуванням доцільності застосування і без будь-якої шкоди продуктивності підприємства. Р.Л. Кіссель трактує як захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, спотворення, зміни або знищення з метою забезпечення конфіденційності, цілісності та доступності. Ю. Черданцева має на увазі мультидисциплінарну сферу досліджень і професійної діяльності, яка зосереджена на розвитку та впровадженні всіляких механізмів безпеки (технічних, організаційних, людиноорієнтованого, юридичних) із метою запобігання інформації від загроз всюди, де б вона не знаходилася (як усередині периметра підприємства, так і за його межами), та, відповідно, інформаційних систем, в яких інформація створюється, обробляється, зберігається, передається і знищується, що, на думку автора, є найбільш повним визначенням.

Під кібербезпекою одні розуміють заходи безпеки, які застосовуються для захисту обчислювальних пристроїв (комп'ютери, смартфони та ін.), а також комп'ютерних мереж (приватних і публічних мереж, включаючи Інтернет). Інші розуміють процес використання заходів безпеки для забезпечення конфіденційності, цілісності та доступності даних. Також автори трактують поняття кібербезпека як сукупність умов, за яких усі складники кіберпростору захищені від максимально можливого числа загроз і впливів із небажаними наслідками. Тобто під кібербезпекою телекомунікаційного підприємства слід розуміти сукупність заходів із захисту мереж, додатків, пристроїв від загроз і впливів внутрішнього і зовнішнього характеру з метою збереження конфіденційності та цілісності даних підприємства для забезпечення коректної роботи.

Використання IT-технологій у діяльності підприємств має свої можливості та загрози. До можливостей можна віднести, наприклад, оперативний доступ до інформації; оптимізацію деяких поточних бізнес-процесів; зменшення витрат підприємства; зростання прибутку; оцінку ефективності роботи співробітника; своєчасне узгодження та прийняття рішення щодо управління підприємством на всіх рівнях управління та різних структурних підрозділах; взаємодію з CRM- та ERP-системами тощо. Однак поряд із можливостями, які надає цифровізація діяльності підприємств, швидко виникають загрози внутрішнього (пов'язані з діями інсайдерів) та зовнішнього (пов'язані зі стейкхолдерами дальнього кола) характеру, що виходять від активів та технологій, використовуваних підприємством. Фахівцями публічної компанії Allianz SE, яка є німецькою фінансовою транснаціональною корпорацією та основним напрямом діяльності якої є страхування, щорічно складається рейтинг бізнесових ризиків. Так, на 2020 р. визначено найбільші глобальні ризики за результатами опитування, заснованого на думці понад 2 700 експертів з управління ризиками з більше ніж 102 країн (табл. 1).

Сумарні відповіді експертів – представників малого та середнього бізнесу становлять близько половини всіх відповідей. Так, для малих підприємств, річ-

Таблиця 1. Десять найбільш глобальних ризиків на 2020 р.

Ризики	Роки			
	2019		2020	
	%	місце у рейтингу	%	місце у рейтингу
Інциденти в кіберпросторі (наприклад, кіберзлочинність, збої/перебої в роботі ІТ, витік даних, штрафи і пені)	37	2	39	1
Переривання бізнесу (включаючи розрив ланцюжка поставок)	37	1	37	2
Зміни в законодавстві та регулюванні (наприклад, торгові війни і тарифи, економічні санкції, протекціонізм, вихід Великобританії з Євросоюзу, розпад Єврозони)	27	4	27	3
Природні катастрофи (наприклад, шторм, повінь, землетрус)	28	3	21	4
Розвиток ринку (наприклад, волатильність, посилення конкуренції/нових учасників, злиття і поглинання, стагнація ринку, коливання ринку)	23	5	21	5
Пожежа, вибух	19	6	20	6
Зміна клімату/підвищення волатильності погоди	13	8	17	7
Втрата репутації або цінності бренду	9	9	15	8
Нові технології (наприклад, вплив штучного інтелекту, автономних транспортних засобів, 3D-друку, Інтернету речей, нанотехнологій, блокчейна)	7	7	13	9
Макроекономічні зміни (наприклад, грошово-кредитна політика, програми жорсткої економії, зростання цін на товари, дефляція, інфляція)	нове	Нове	11	10

Джерело: складено автором на основі даних [4]

Таблиця 2. П'ять найбільших ризиків на 2019 р. для малих підприємств

Ризики	Роки			
	2018		2019	
	%	місце у рейтингу	%	місце у рейтингу
Інциденти в кіберпросторі (наприклад, кіберзлочинність, збої/перебої в роботі ІТ, порушення даних, штрафи і штрафи)	30	2	32	1
Зміни в законодавстві та регулюванні (наприклад, торгові війни і тарифи, економічні санкції, протекціонізм, вихід Великобританії з Євросоюзу, розпад Єврозони)	22	5	30	2
Природні катастрофи (наприклад, шторм, повінь, землетрус)	28	3	27	3
Розвиток ринку (наприклад, волатильність, посилення конкуренції/нових учасників, злиття і поглинання, стагнація ринку, коливання ринку)	27	4	27	4
Переривання бізнесу (включаючи розрив ланцюжка поставок)	33	1	26	5

Джерело: складено автором на основі даних [6]

Таблиця 3. П'ять найбільших ризиків на 2019 р. для середніх підприємств

Ризики	Роки			
	2018		2019	
	%	місце у рейтингу	%	місце у рейтингу
Переривання бізнесу (включаючи розрив ланцюжка поставок)	37	2	38	1
Інциденти в кіберпросторі (наприклад, кіберзлочинність, збої/перебої в роботі ІТ, порушення даних, штрафи і штрафи)	39	1	32	2
Природні катастрофи (наприклад, шторм, повінь, землетрус)	32	3	29	3
Зміни в законодавстві та регулюванні (наприклад, торгові війни і тарифи, економічні санкції, протекціонізм, вихід Великобританії з Євросоюзу, розпад Єврозони)	18	6	24	4
Розвиток ринку (наприклад, волатильність, посилення конкуренції/нових учасників, злиття і поглинання, стагнація ринку, коливання ринку)	21	5	23	5

Джерело: складено автором на основі даних [6]

ний дохід яких становить менше ніж 250 млн євро, головним ризиком є інциденти в кіберпросторі, що в 2019 р. збільшився на 2% порівняно з 2018 р. Для середніх підприємств, річний дохід яких становить від 250 до 500 млн євро, найбільшим ризиком є переривання бізнесу (включаючи розрив ланцюжка поставок) (табл. 2 та 3).

Узагальнюючи проаналізовані найбільші ризики останніх років, інциденти у кіберпросторі переважають над усіма іншими ризиками та спричиняють необхідність їх систематизації й формування основ щодо управління ними. Спробу систематизувати кіберризики підприємства зовнішнього та внутрішнього характеру зроблено у [5]. Слід відзначити, що

до зовнішніх ризиків належать нецільові (фішинг, кардинг, sms шахрайство) та цільові (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS-атаки, кібервимагання) атаки. Місцями загроз (уразливості) телекомунікаційного підприємства є системи управління підприємствами (наприклад, автоматизована система керування підприємством, ERP-системи), системи комунікації з клієнтами (наприклад, CRM-системи), фінансова звітність, Інтернет-банкінг, дистанційне банківське обслуговування, автоматизовані системи управління технологічними процесами та системи візуалізації (наприклад, SCADA), прикладні вебпрограми (наприклад, мобільні додатки), портали, Інтернет-магазини, платіжні електронні системи та інші місця. При цьому втрати можуть бути як прямі (вкрадені кошти), так і опосередковані (простій окремих бізнес-процесів або підприємства у цілому, втрата даних).

Під час своєї діяльності підприємства використовують різноманітні технології з метою автоматизації можливих процесів та полегшення ведення бізнесу. Але існують загрози, що пов'язані з діями інсайдерів (особа, яка має доступ до важливої/конфіденційної інформації про діяльність підприємства, недоступної широкому колу людей), наприклад порушення цілісності та достовірності інформації, викрадення персональних даних, витік інформації через необачливість, неавторизований доступ, маніпуляції з програмним забезпеченням, несанкціоноване встановлення програмного забезпечення, використання шахраями методик соціальної інженерії (методики маніпуляції, які допомагають змусити людину віддати зловмисникам необхідні дані), зловживання повноваженнями тощо.

Уразливими елементами ТП, які можуть постраждати внаслідок кіберінциденту, є бізнес-процеси підприємства, його інфраструктура, нематеріальні та матеріальні активи, використовувані технології, репутація та вартість бізнесу. Будь-яке ураження цих елементів призведе до компрометації ТП та некоректної його роботи, що веде до простоїв і втрат частини прибутку, споживачів, частки ринку, партнерів й витрачання додаткових коштів на покриття збитків, пов'язаних із відновленням внутрішньої (зовнішньої) інфраструктури.

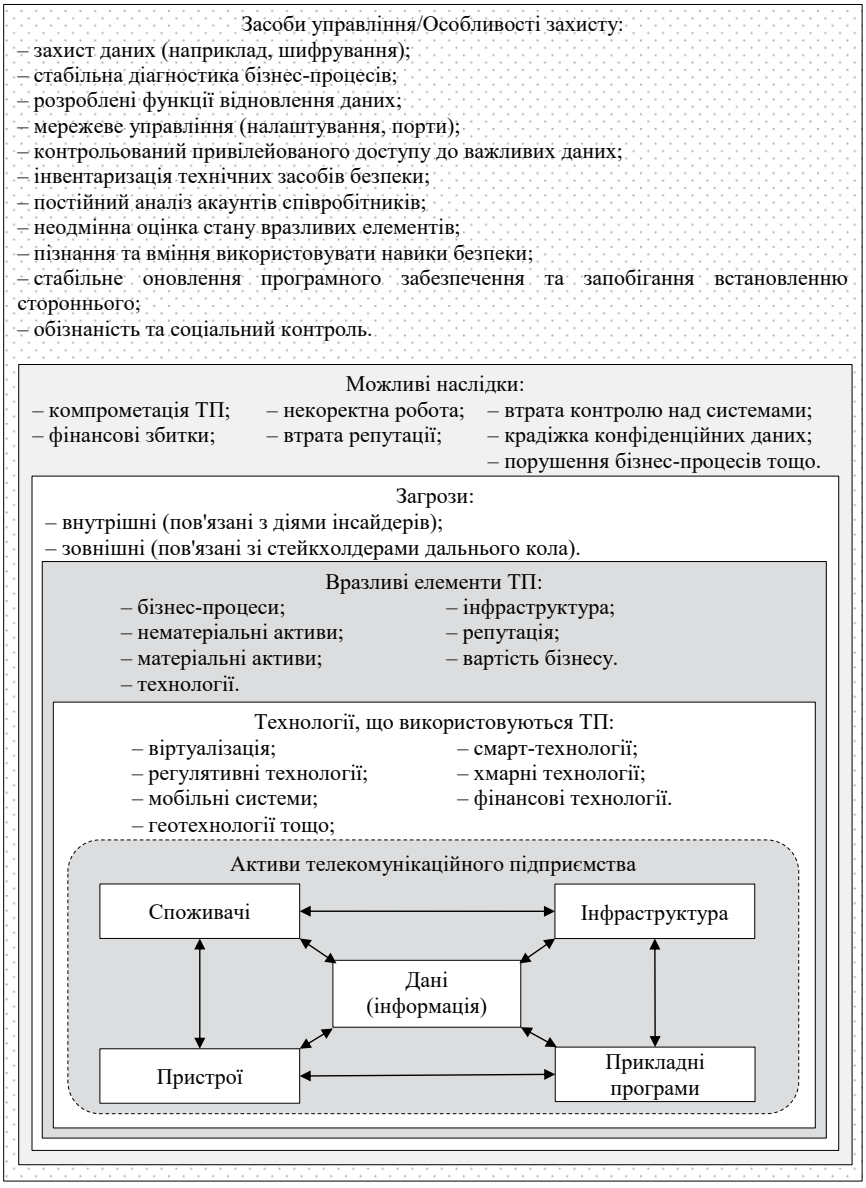

Рис. 1. Процесний підхід до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів

Джерело: власна розробка автора

Таким чином, узагальнюючи все вище сказане, автором представлено процесний підхід до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів (рис. 1), який засновано на дослідженні технологій, що використовуються таким підприємством, визначенні його вразливих елементів під час діджиталізації з виявленням загроз та можливих наслідків, які впливають на активи, а також представлено засоби управління/особливості захисту. Кіберризики мають свої особливості, певні види подій і можливі збитки та на відміну від традиційних ризиків можуть наздогнати бізнес у будь-якій точці світу і практично в кожному бізнес-процесі. Кіберризик визначається як комбінація ймовірності інциденту у сфері інформаційної системи і впливу цього інциденту на активи та є бізнес-проблемою з технічними аспектами. Кіберризики ґрунтуються на нанесенні шкоди активам підприємств, які, своєю чергою, потребують адекватних та надійних засобів управління, наприклад захисту даних (шифрування); стабільної діагностики бізнес-процесів; розроблення функції відновлення

даних; мережевого управління (налаштування, порти); контрольованого привілейованого доступу до важливих даних; інвентаризації технічних засобів безпеки; постійного аналізу акаунтів співробітників; неодмінної оцінки стану вразливих елементів; пізнання та вміння використовувати навики безпеки; стабільного оновлення програмного забезпечення та запобігання встановленню стороннього; обізнаності та соціального контролю тощо.

Усе вищесказане спричиняє необхідність установлення ступеню кіберризику (низького, помірного, значного, високого) з метою розроблення та впровадження керівництвом підприємства відповідних дій їх мінімізації залежно від каналів джерел кіберзагроз та видів ризику (табл. 4).

Загрози мають такий характер, що ніхто не може дати стовідсоткової гарантії захищеності, оскільки підприємства працюють в умовах підвищеної швидкості появи нових технологій і кіберзагроз підвищується в результаті еволюційного розвитку системи захисту інформації від «безперервності ІТ» до «інформаційної безпеки» і далі до «кібербезпеки», виникло поняття кіберсталості (кіберстійкості) підприємства.

Однією з перших спроб уведення поняття «кіберстійкість» здійснено в роботі [7], де містяться формальні математичні визначення з використанням теорії множин. Інші трактують це поняття як здатність компанії бути готовою до кібератаки, швидко приймати рішення під час атаки, готовності до постійного

Таблиця 4. Канали джерел кіберзагроз, види та ступінь кіберризику телекомунікаційного підприємства

Канали джерел кіберзагроз		Види кіберризику					
		Фінансове шахрайство	Викрадення даних споживачів	Порушення бізнес-процесів	Втрата конфеденційності інтелектуальної власності	Руйнування внутрішньої та зовнішньої інфраструктури	Ускладнення вчинення регуляторних дій
внутрішні	Доступ до важливої інформації						
	Маніпуляції з програмним забезпеченням						
	Зловживання повноваженнями						
	Соціальна інженерія						
зовнішні	Партнери						
	Конкуренти (корпоративне шпигунство)						
	Незадоволені споживачі						
	Хакерські угрупування						
	Форс-мажорні обставини						

	низький		помірний		значний		високий

Джерело: сформовано автором

впливу кіберзагроз та забезпечення захисту інформаційної безпеки превентивними мірами є застарілою, оскільки ціллю є виявлення атаки або її наслідків як можна раніше. У таких умовах, коли мінімізуючи збиток від неї та її тривалість, а також швидко і з мінімальними втратами відновлюватися після атак. Згідно з [8], у контексті безпеки кіберстійкість означає здатність підприємства підтримувати свої основні функції і цілісність за впливу потенційних атак із загрозою її інформаційної безпеки. При цьому кіберстійка компанія розглядається як компанія, що здатна запобігати, виявляти, стримувати атаки і відновлюватися після них, мінімізуючи свою схильність атаці та її впливу на бізнес, тобто протистояти незліченній кількості загроз даних, додатків та IT-інфраструктури, але особливо загроз пристроїв, де знаходяться найцінніші інформаційні активи підприємства, тому що їх поразка означатиме також порушення недоторканності підприємства і співробітників.

Сучасні цифрові платформи, які у своїй діяльності використовують підприємства, не мають достатнього рівня кіберстійкості через високу структурну та функціональну складність, тому телекомунікаційним підприємствам, що впроваджують новітні технології, необхідно створювати «імунну систему» підприємства за допомогою програмного забезпечення з використанням штучного інтелекту та нейронних мереж, оскільки саме вони мають здатність до самонавчання, працювати швидше людини, постійно розвиватися та спроможні швидко вирішувати виникаючі завдання, підключаючись до хмарних технологій, які надають необхідні ресурси.

Для того щоб «імунна система» телекомунікаційного підприємства була цілісною, передусім необхідно, щоб його керівні органи дотримувалися певних принципів через інтеграцію кіберстійкості до бізнес-стратегії з метою уможливлення інноваційного, надійного та збалансованого зростання. Тож першим принципом є відповідальність керівних органів за кіберстійкість із можливістю делегування первинної наглядової діяльності за кіберризиками та кіберстійкістю підрозділу з кібербезпеки, співробітники якого мають достатні повноваження, регулярний доступ до керівництва, володіють предметом, досвідом та ресурсами для виконання таких обов'язків. Керівні органи підприємства регулярно інформуються про останні загрози та тенденції через консультації незалежних експертів.

Не менш важливим питанням у дослідженні інформаційної безпеки, стійкості та загроз є можливість оцінки збитків телекомунікаційного підприємства від кіберінциденту, оскільки від коректної та захищеної роботи залежить не тільки воно само, а й усі його споживачі. Загалом можливий збиток можна поділити на фінансовий та майновий, а витрати, пов'язані зі збитком, – на прямі та непрямі (табл. 5).

Пропонована матриця оцінки збитків телекомунікаційного підприємства від кіберінциденту з розподілом на фінансовий на майновий дасть змогу з'ясувати ступінь пошкодження матеріальних та нематеріальних активів як самого підприємства, так і споживачів його послуг. Для мінімізації або усунення кіберризиків існує три основних напрями: технологічні рішення безпеки, просвітницька робота у сфері протидії та профілактики кіберзлочинів, а також кіберстрахування, яке дає змогу не тільки передати частину ризику на страхування, а й забезпечити покриття можливих збитків.

Висновки з проведеного дослідження. Спираючись на проведені дослідження, інформаційну безпеку підприємства слід розглядати як проблему управління не тільки інформаційними ризиками, пов'язаними з інформаційними технологіями, а й як проблему управління корпоративними ризиками для захисту власних активів найбільш ефективними засобами на основі застосування адаптивного, комплексного та сумісного підходу, що також підтверджується аналітичними даними. Автором представлено процесний підхід до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів, що спирається на визначення вразливих елементів під час діджиталізації підприємства із виявленням загроз та можливих наслідків, які впливають на активи, із виділенням засобів управління/особливостей захисту з метою визначення важелів

Таблиця 5. Матриця оцінки збитків телекомунікаційного підприємства від кіберінциденту

	Прямі витрати ТП	Витрати відповідальності ТП
Фінансовий збиток	1) витрати пов'язані із реагуванням на кіберінцидент (IT-розслідування, повідомлення споживачів про компрометацію ТП); 2) юридична допомога з питань вимог від постраждалих споживачів та судові витрати; 3) витрати з мінімізації репутаційного збитку; 4) втрати прибутку через вплив на рівень продажів послуг, частку ринку, цін на акції підприємства; 5) витрати на відновлення даних / коректної роботи / інфраструктури / системи управління; 6) витрати на відновлення конфіденційності інтелектуальної власності тощо.	1) покриття втраченої вигоди споживачами; 2) витрати на відновлення функціональності споживачів; 3) витрати пов'язані із правовою допомогою; 4) фінансові збитки та збитки, які понесені від втрати даних; 5) накладені штрафи тощо.
Майновий збиток	1) викрадення активів; 2) виведення обладнання з ладу внаслідок кіберінциденту; 3) знищення або заподіяння шкоди будівлям, спорудам, іншому майну; 4) перерви у діяльності; 5) заподіяна шкода безпеці життя та здоров'ю співробітників тощо.	1) викрадення активів споживачів; 2) виведення обладнання споживачів із ладу внаслідок кіберінциденту; 3) знищення або заподіяння шкоди будівлям, спорудам, іншому майну споживачів; 4) завдання шкоди навколишньому середовищу; 5) заподіяна шкода безпеці життя та здоров'ю споживачів або третіх осіб тощо.

Джерело: сформовано автором

мінімізації глобальних та локальних інформаційних ризиків. Підприємства телекомунікацій повинні постійно контролювати використовувані корпоративні процеси, технології, інструменти та сервіси безпеки і проводити коректувальні дії у міру розвитку та зростання загроз у процесі постійного вдосконалення та збалансованого розвитку, заснованого у тому числі на обережності та адаптації у мінімальні строки з максимальною швидкістю.

Умови підвищеної готовності до постійного впливу кіберзагроз та забезпечення захисту інформаційної безпеки телекомунікаційним підприємствам необхідно встановлювати ступень кіберризику залежно від каналів джерел кіберзагроз та видів ризику для розроблення й упровадження керівництвом підприємства відповідних дій щодо їх мінімізації. Для оцінки збитків від кіберінциденту автором запропоновано матрицю 2x2, що розподіляє збиток на фінансовий і майновий, а витрати розподіляються на прямі витрати та витрати відповідальності перед третіми особами, що дає змогу встановити ступінь пошкодження матеріальних та нематеріальних активів як самого підприємствами, так і споживачів його послуг.

Перспективою досліджень є визначення основних напрямів мінімізації або усунення глобальних та локальних інформаційних ризиків шляхом застосування світових технологічних рішень, профілактики, передачі частини ризиків на страхування тощо.

Список використаних джерел:

1. Проєкт «Цифрова адженда України – 2020». URL : https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (дата звернення: 14.02.2020).

2. Україна 2030: Доктрина збалансованого розвитку ; вид. 2-е. Львів : Кальварія, 2017. 164 с.

3. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016. Дата оновлення: 15.03.2016. URL : https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 14.02.2020).

4. Allianz Global Corporate & Specialty SE. Allianz Risk Barometer Top Business Risks 2020. URL : https://www.agcs.allianz.com/content/dam/ onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf (дата звернення: 14.02.2020).

5. Demyanchuk M., Maslii N., Stankova V. Cyber-insurance as a tool for minimizing the informational risks of the enterprise in the conditions of global economic development and society informatization. *Економіка: реалії часу.* 2018. № 5(39). С. 41–51. DOI : 10.5281/zenodo.2570060.

6. Allianz Global Corporate & Specialty SE. Allianz Risk Barometer Top Business Risks 2019. URL : https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf (дата звернення: 14.02.2020).

7. Promyslov V.G., Poletykin A.G. Formal Hierarchical Model of Security of the Upper Level of Instrumentation & Control System of a Nuclear Power Plant. *Proceedings of the 7th IFAC Conference on Manufacturing Modelling, Management, and Control* (MIM`2013, Saint Petersburg). Saint Petersburg: International Federation of Automatic Control (IFAC), 2013. T. 1. URL : http://www.ifac-papersonline.net/Detailed/60537.html. (дата звернення: 14.02.2020).

8. Саммит Panda Security Summit. Кибер-устойчивость: ключ к безопасности компании. URL : https://www.cloudav.ru (дата звернення: 14.02.2020).

References:

1. HiTech office (2016) Proekt «Tsyfrova adzhenda Ukrainy – 2020» [Project "Digital Agenda of Ukraine – 2020"]. Available at: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (accessed 14 February 2020).

2. Kal'variia (2017) Ukraina 2030: Doktryna zbalansovanoho rozvytku [Ukraine 2030: The Doctrine of Balanced Development]. L'viv: Kal'variia.

3. *Ukaz Prezydenta Ukrainy Pro ctratehiiu kiberbezpeky Ukrainy* [Presidential Decree On Ukraine's Cybersecurity Strategy] № 96/2016 (2016, March 15). Available at: https://zakon5.rada.gov.ua/laws/show/96/2016 (accessed 14 February 2020).

4. Allianz Global Corporate & Specialty SE. *Allianz Risk Barometer Top Business Risks 2020.* Available at: https://www.agcs.allianz.com/content/dam/ onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf (accessed 14 February 2020).

5. Demyanchuk M., Maslii N., Stankova V. (2018) Cyber-insurance as a tool for minimizing the informational risks of the enterprise in the conditions of global economic development and society informatization. *Economics: time realities.* Odessa. № 5(39). pp. 41–51. DOI: 10.5281/zenodo.2570060.

6. Allianz Global Corporate & Specialty SE. *Allianz Risk Barometer Top Business Risks 2019.* Available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf (accessed 14 February 2020).

7. Promyslov V.G., Poletykin A.G. (2013) Formal Hierarchical Model of Security of the Upper Level of Instrumentation & Control System of a Nuclear Power Plant. *Proceedings of the 7th IFAC Conference on Manufacturing Modelling, Management, and Control* (MIM`2013, Saint Petersburg). Saint Petersburg: International Federation of Automatic Control (IFAC). T. 1. Available at: http://www.ifac-papersonline.net/Detailed/60537.html. (accessed 14 February 2020).

8. Panda Security Summit. *Kiber-ustojchivost': kljuch k bezopasnosti kompanii* [Cyber Resilience: Key to Company Security]. Available at: https://www.cloudav.ru (accessed 14 February 2020).

E-mail: ma-demyanchuk@ukr.net