ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 007:004.56:616-036.21.2019

[0000-0002-8555-5712] **М. Д. Василенко,** *д.ф.-м.н., д.ю.н., професор, в.о. завідувача кафедри кібербезпеки*,
e-mail: nvas08@ukr.net
[0000-0003-2059-0581] **В. П. Новіков,** *к.т.н., доцент, доцент кафедри кібербезпеки*,
e-mail: novikovodessa0@gmail.com
[0000-0003-1793-016X] **В. О. Рачук,** *асистент кафедри кібербезпеки*,
e-mail: rachuk960@gmail.com
[0000-0002-6082-981X] **В. М. Слатвінська,** *аспірантка кафедри господарського права та процесу,*
e-mail: slatvinskaya_valeriya@ukr.net
Національний університет «Одеська юридична академія»
Фонтанська дорога, 23, м. Одеса, 65009, Україна

КІБЕРБЕЗПЕКА В ПРОЯВАХ РИЗИКІВ У ПЕРІОД ПАНДЕМІЇ: СТАН ТА ГЕНЕЗА

Стаття покликана стимулювати інтерес до проявів ризиків у кібербезпеці в умовах COVID-19 (коронавірусу). Зокрема, проаналізовано та надано оцінку проявам кіберризиків у контексті кібербезпеки як нової проблеми, пов'язаної з появою COVID-19, а також з'ясовано її стан та генезу. Запропоновано вирішити проблему управління різними видами ризиків шляхом інституційного розуміння забезпечення юридичного підґрунтя та багатофакторного проєктування або прогнозування, а також запропоновано основний метод посилення захисту – технічний, що використовує, перш за все, алгоритмічні методи, а в окремих випадках – можливість використання сил «Червоної команди» захисної структури. Показано, що в умовах принципового збільшення телеконференцій (у період пандемії) суттєво збільшується кількість кіберризиків. Зазначено основні заходи безпеки, потрібні для захисту інформаційно-комунікативної інфраструктури в умовах дії пандемії по COVID-19 (коронавірусу). Авторами доведено, що, оскільки ризики все більше стають послідовними та взаємопов'язаними процесами як невід'ємні складники системи управління, то в цьому випадку більш доречними стають періодичні перевірки офісних приміщень на виявлення використання технічних засобів скритого зняття інформації та періодичне проведення онлайн семінарів зі співробітниками з питань безпеки.

Ключові слова: *кібербезпека, ризик, оцінювання ризику, невизначеність, пандемія, COVID-19.*

Вступ. Епідемія коронавірусу (COVID-19), що створила безпрецедентну глобальну надзвичайну ситуацію, стала серйозним тестом для урядів, громадян та економік більшості країн світу, які підпали під серйозні ризики. Так, за даними Центру скарг на інтернет-злочини (ЦСІЗ) ФБР (США), наведеними у звіті про злочинність в Інтернеті за 2019 рік, злочини та шахрайства з використанням всесвітньої мережі не мають жодних ознак щодо їх припинення, а мають тенденцію до стрімкого збільшення. ЦСІЗ зафіксував за останній рік збитки у розмірі майже чотири мільярди доларів для приватних осіб і постраждалого бізнесу [1]. Аналіз інформації, яка надходить з країн-членів ЄС, також підтверджує той факт, що в результаті пандемії з великим відсотком ймовірності очікуються ризикові економічні й політичні негаразди. З появою коронавірусу додаткові проблеми з'явилися майже в усіх країнах і в усіх владних структурах, а урядові рекомендації, що стосувалися COVID-19, привели до безпрецедентного переходу на онлайн-роботу. За цих виняткових обставин невирішеною важливою проблемою залишається забезпечення зниження ризиків загалом і кіберризиків зокрема. Через те, що під час пандемії безперервна діяльність в основному відбувається завдяки використанню віддалених операцій, у світі з'явилася величезна кількість «фішингових» кампаній. Загальновідомо, що фішинг являє собою різновид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів. Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень усередині різних сервісів, наприклад від імені банків, або усередині соціальних мереж. У листі часто

DOI: 10.24025/2306-4412.3.2020.214774

міститься пряме посилання на сайт, який зовні важко відрізнити від реального, або на сайт з редиректом. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленій сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дає шахраям можливість отримати доступ до облікових записів та банківських рахунків. У той час як сьогодні в багатьох країнах запроваджують заходи, щоб допомогти жертвам COVID-19 і обмежити зараження, хакери використовують кризу та продовжують свої дії для здійснення цілеспрямованих кібератак на підприємства, зокрема на робочі місця. У період кризи хакери намагаються використовувати увагу, яку приділяють вірусам, і пов'язаний з ними панічний ефект для проведення фішингових кампаній, видаючи себе за сповіщення, пов'язані з COVID-19 (див. [2]). Отже, майже всі випадки можливих загроз базуються на розумінні та використанні ризиків і ризикових ситуацій.

Аналіз публікацій та джерел досліджень/дослідження. З багатьох публікацій щодо дослідження ризиків у вітчизняних та іноземних виданнях відомо безліч визначень «ризику», що допускає досить широке його тлумачення. Так, тільки в Інтернет-словниках містяться сотні тлумачень ризику у багатьох сферах, допомагаючи розкривати сутність самого ризику та пов'язаних з ним понять [3]. Праць, присвячених суто кібербезпеці, також досить багато, включаючи ті, в яких досліджуються питання кіберризиків. Однак праць, в яких йдеться про вирішення цих проблем у кіберсередовищі в період пандемії, дуже мало. Насамперед, відзначимо працю співавторів цієї статті, де досліджувалися проблеми кіберризиків в умовах комунального буття в господарствах міст у період пандемії [2]. На основі зазначеного першоджерела необхідно дослідити, як вплинула ситуація з пандемією на стан кібербезпеки та кіберризиків. Також відзначимо наукові праці (див. [4], [5], [6], [7]), в яких йдеться, зокрема, про онлайн-роботу вдома під час COVID-19, заходи в галузі кібербезпеки під час пандемії та кібератаки на так звані «смарт-будинки». Проте наразі ми не можемо використати наведені актуальні дослідження з огляду на те, що нас цікавить, яким чином пандемія вплинула на наявний рівень кібербезпеки.

Новизна означеної статті полягає в аналізі розширення «поверхні атаки», яке відбулося через пандемію, коли користувачі Інтернету масово заполонили інтернет-ресурси, що дало: (а) з технічного боку – більше сервісів, схильних до вразливостей, при розширенні сервісів, щоб відповісти на запити ринку, безпеці приділялося недостатньо уваги, що спричинило збільшення атак; (б) з соціального боку – більше приводів для фішингу. А це, в свою чергу, привело до того, що в умовах нових проблем сучасності під час пандемії необхідно запропонувати їх практичне вирішення.

Метою дослідження є аналіз і оцінювання генези та проявів кіберризиків як нової проблеми функціонування кіберпростору, пов'язаної з появою COVID-19 (коронавірусу).

Виклад основного матеріалу. Поняття «ризик» має досить широке трактування. Водночас його соціальна сутність полягає, перш за все, в тому, що суб'єкт, свідомо відступаючи від встановлених у суспільстві правил поведінки, створює конфліктну ситуацію, загострює проблему до межі і, використовуючи переваги екстремальної ситуації, прагне вирішити поставлене завдання, яке найчастіше має негативний сенс. Тому зрозумілими стають ймовірні ризики від дій непрофесійних керівників, які вважають себе «ефективними менеджерами».

Відповідно, такий стан характерний також і для сфери інформаційної безпеки та елементів і засобів кібернетики, яка наразі впроваджена в будь-яку систему управління. У зв'язку з цим аналіз і розкриття поняття «ризику» для його подальшої інтерпретації розширить можливості з підвищення ефективності ще й інформаційної безпеки. Враховуючи, що ризики стосуються різних предметних галузей, це поняття слід розглянути з точки зору безпеки, психології, економіки, медицини тощо. Воно показано як у безлічі публікацій, так і в різних нормативних документах (див., наприклад, [8]). Втім, виникає проблема управління різними видами ризиків, що потребує, на нашу думку, інституційного розуміння. Крім того, для розв'язання, наприклад, управлінських завдань слід визначитися з використанням прогнозування (оцінювання) ризиків. Нерідко для цього автори виходять із позицій кібернетичного бачення явища та кібернетики в цілому, яка, за визначенням академіка В. М. Глушкова, являє собою «науку

DOI: 10.24025/2306-4412.3.2020.214774

про загальні закони одержання, зберігання, передавання й перетворення інформації у складних системах управління» [9].

Визначення ризику містяться в багатьох нормах різних галузей господарства і техніки. Однак існує Міжнародний стандарт ISO 31000 [10], який використовується для загального оцінювання ризику. Щоб реалізовувати процес керування ризиком, він має бути інтегрованим зі складовими керування ризиками, що включає обмін інформацією та консультування; встановлення контексту (оточення); загальне оцінювання ризику (його ідентифікація, аналіз та оцінювання); оброблення та узагальнення отриманих результатів обраного типу ризику; моніторинг і критичне аналізування.

Міжнародний стандарт ISO 31000 враховує, в цілому, більшу частину можливих ризиків та пов'язаних із ними складових, у тому числі й епідемічних ризиків. З позиції загальної теорії ризиків слід звернути увагу на принципову особливість, а саме на те, що «прогнозуванням» часто замінюють «оцінювання» ризиків. Якісне прогнозування, як, наприклад, метод експертних оцінок, використовують у нетехнічній сфері, і тут воно, схоже, функціонує аналогічно оцінюванню. Однак між ними існує різка відмінність у стандартній моделі статистичного оцінювання. Так, у гуманітарних науках частіше говорять про обґрунтований ризик, що не викликає зауважень з нашого боку. Обґрунтований ризик слід відмежовувати від спричинення шкоди в стані крайньої необхідності, коли для деяких категорій осіб дія в стані крайньої потреби поставлена в обов'язок, а ризик виступає як виключно суб'єктивне право будь-якого суб'єкта. У разі крайньої необхідності спонукальним мотивом дій суб'єкта є загрозлива небезпека суспільно значущим інтересам, а при ризику – досягнення соціально значущої мети. За умов крайньої необхідності, наприклад пандемії, критеріями порівняння є: тяжкість шкоди, заподіяної зловмисниками, та запобігання їй з урахуванням витрат, а при підвищеному ризику акцент робиться на порівнянні ступеня вірогідності спричинення шкоди (наприклад гранично допустимий ризик тяжких наслідків, але з мінімальним ступенем вірогідності).

В інформаційних технологіях, які забезпечують нормальну (безперешкодну) роботу інформаційно-комунікаційної інфраструктури, ризики мають більш суттєве значення, визначаючи реально виражену конкретику. За даними Інтернет-спільноти, в період пандемії з COVID-19 зросла кількість атак на інформаційні ресурси таких інфраструктур. Точних цифр авторам віднайти не довелося, але приблизна оцінка зростання кількості атак, найімовірніше, перебуває в діапазоні (15–25) % [2].

Зростання у суспільстві паніки, яка пов'язана з розповсюдженням COVID-19, стало приводом як для появи нових кіберризиків, так і посилення старих шахрайських дій та інших негативних проявів. Задля цього шахраї вставляють шкідливі програми, які ставлять під загрозу пристрої користувачів та їхню особисту інформацію. Коли співробітники органів самоврядування, державних та господарських структур працюють вдома (онлайн), а їх пристрої підключені до віддалених серверів, під загрозу підпадають як зазначені прилади, так і вся інформаційна структура і сама мережа в цілому. Досить широко розповсюджені вже зазначені вище «фішингові» повідомлення (листи) з профілактики і лікування COVID-19, які, начебто, направлені від державних установ або органів охорони здоров'я. Одним із найпростіших і популярних методів фішинг-атак став спосіб, коли зловмисники вказують у темі листа назву вірусу COVID-19, і людина відкриває його, інфікуючи свій пристрій. В цілому, відзначимо, що таке кібершахрайство набуло стрімкого та стійкого зростання майже в усіх країнах.

В умовах необхідності створення безпеки в інформаційно-комунікаційних системах оцінювання та якісний аналіз інформаційних ризиків дають можливість визначити необхідний рівень захисту інформації, здійснити його підтримку і розробити стратегію розвитку інформаційної структури системи. Мається на увазі, що це стосується самої компанії або підприємства. Оцінювання та аналіз інформаційних ризиків виступають необхідною умовою при створенні системи керування ризиками і формуванні плану забезпечення стабільної роботи підприємства, а також при забезпеченні безперервності роботи та відновлення бізнесу. В широкому сенсі, у разі дослідження інформаційної безпеки, ризик часто відображається імовірністю функціонально (стохастично) пов'язаних з нею понять. У цьому випадку можливий вимір результату визначається ймовірністю матеріальних та інших втрат через вірогідність появи несприятливого результату

DOI: 10.24025/2306-4412.3.2020.214774

або події. Трапляється також визначення ризику як дії або діяльності, реалізація якої ставить під загрозу задоволення будь-якої досить важливої потреби. В окремих джерелах ризик трактується як міра небезпеки, що характеризує ймовірність її появи й розміри пов'язаної з нею шкоди. Трапляються і визначення ризику, які зображують його як небезпеку вибору з двох або більше альтернативних варіантів дій і передбачають хоча б мінімальне збереження вже досягнутого раніше.

При дослідженні технічних ризиків виділяють їх базові витоки: ризик розглядають як вимірювану або розраховану в деяких межах ймовірність отримання можливих результатів; ризик пов'язують з настанням певної події (як правило, несприятливої); поняття ризику розкривається через практичну діяльність суб'єкта; ризик розкривається через не залежну від суб'єкта діяльності подію, настання якої кількісно можливо оцінити; водночас часто акцент робиться на кількісному та якісному оцінюванні ризику – «мірі ризику»; поняття «ризику» розкривається через невизначеність; ризик відображається ситуацією можливості вибору з двох або з певної визначеної множини варіантів дії; ризик сприймається як небезпека, частота витрати і втрати, всебічна характеристика ситуації, а також комплексний аналіз деякого функціоналу, заданого на множині вірогідних значень (деякої сумарної величини). В цьому разі при обговоренні поняття «ризику» можна виділити одну характеристику, яка є в усіх визначеннях, наведених вище, та об'єднує їх. Це є ніякий функціонал події, яка має відбутися і яка пов'язана з імовірністю, дією або діяльністю, мірою, частотою, вибором певних рішень, невизначеністю, з втратами, небезпекою і т. д. Водночас саме управління ризиками розглядають як процес ідентифікації, управління, усунення або зменшення ймовірності подій, здатних негативно впливати на ресурси інформаційної системи, зменшення ризиків безпеки, що потенційно мають можливість впливати також на інформаційну безпеку, за умови прийнятної вартості засобів захисту. Управління ризиками містить всі операції, які можна проводити над ризиком інформаційної безпеки: мінімізація, нейтралізація, прийняття очікуваної частки ризику, передача ризику або страхування.

Аналіз та оцінювання ризику визначають послідовними взаємопов'язаними процедурами, які входять у процес управління. Оцінювання ризику розглядається як процес ідентифікації визначальних параметрів інформаційних ресурсів системи і загроз цим ресурсам, а також можливих втрат, що ґрунтуються на оцінюванні частоти виникнення подій і розміру збитку. Аналіз ризику розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що вимагають захисту. Отже, прийняття раціональніших рішень у цих випадках вимагає використання специфічного математичного апарату теорії статистичних рішень, нейронних мереж, генетичних алгоритмів, теорії ігор. Цільова невизначеність виникає у багатоцільових завданнях, які потребують багатокритеріального вибору та оптимальних рішень, а оцінювання ризику передбачає дослідження стану, ситуації (сценаріїв) з наявними ознаками небезпеки, невизначеності та/або випадковості. Найефективнішим методом його здійснення є забезпечення юридичного підґрунтя та багатофакторне проєктування або прогнозування. На етапі оцінювання ризиків формується стратегія управління ризиками, а оскільки повністю уникнути ризиків у більшості випадків неможливо, то вагоме значення має вирішення питання допустимості (прийнятності, виправданості) ризику, яке потребує подальшого дослідження та обґрунтування. Оцінювання ризику, що використовують у технічних системах, розглядається як процес ідентифікації інформаційних ресурсів системи і загроз цим ресурсам, а також можливих втрат, що базується на оцінюванні частоти виникнення подій і розміру збитку. Аналіз ризику розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що потребують захисту. На прикладі впливу обмежувально-карантинних заходів на навчальний процес, а саме введення в дію дистанційного навчання засобами телеконференцій через Інтернет-мережі, з'явився ще один напрям ризику, що спричинений самим реальним фактом значного підвищення активності користувачів безпосередньо в мережі Інтернет.

Популярність та капіталізація сервісу відеоконференцій в десятки разів зросла з початком пандемії коронавірусу. При спілкуванні автоматично активізуються інтернет-

DOI: 10.24025/2306-4412.3.2020.214774

злочинці, інтернет-шахраї, закономірно, що зростає загроза в кіберпросторі.

Пов'язані з коронавірусною пандемією карантинні заходи та режими самоізоляції привели до різкого зростання різних онлайн-сервісів – до них входять, у тому числі, онлайн-магазини, онлайн-послуги різного роду і сервіси онлайн-зв'язку (зокрема онлайн-конференції). Багато сервісів запускалися і масштабувалися без урахування заходів безпеки – в спробі довести пропозицію до рівня стрімко висхідного попиту. Це призвело до розширення «поверхні атаки» – можливостей для широкого спектра атак, а масштабування і запуск нових сервісів призвели до проявів нових вразливостей. Результатом цього було різке зростання кіберзлочинів, що корелює зі зростанням попиту на онлайн-сервіси.

Найбільш гучні атаки відбулися на систему онлайн-конференцій Zoom, коли під час пандемії кількість таких конференцій збільшилася в десятки разів. В [11] описується вразливість у Zoom, в якій був залучений помилковий анімований GIF-файл. 18 травня 2020 року стався масштабний вихід з ладу безлічі серверів Zoom на кілька годин. Як з'ясувало розслідування інциденту по гарячих слідах, зловмисники зареєстрували безліч помилкових адрес, афілійованих з Zoom, і скористалися ними для фішингу, що спричинило масштабний витік особистих даних користувачів системи (зокрема логінів і паролів). Надалі ці дані були використані в безлічі інших атак – зокрема 12 травня було зламано трансляцію церемонії випускників Оклахомського університету. Ще до інциденту було виявлено безліч неприємних подробиць стосовно організації захисту Zoom, точніше того, які ключові ланки в ній відсутні. Зокрема представники Zoom у березні визнали, що система не використовує "end-to-end" шифрування, відповідно, у зловмисників буде доступ до персональних даних користувачів, якщо вони будь-яким чином отримають доступ до серверів компанії.

З'явився новий тип фішингових розсилок, який використовує коронавірусні теми – зокрема маскується під центри контролю захворювань [12], сервіси та додатки, що дають змогу відстежувати епідемічну картину, і навіть пропозиції про спільне виробництво ізоляційних масок [13]. При цьому як «носій» у рамках kill-chain можуть використовуватися як нові, так і «перевірені» представники шкідливого програмного забезпечення. Наприклад, за звітами центру реагування на інциденти інформаційної безпеки (CERT-GIB) [12], більшу частину фішингових листів становлять програми-шпигуни і бекдори – сумарно 96 %, залишок припадає на шифрувальники. Найчастіше використовуються трояни AgentTesla (45 %), Netware (30 %) і LokiBot (8 %).

Навіть якщо взяти тільки програми відеоконференцій, які в інтернет-просторі зарекомендували себе з найкращої сторони: Zoom, Skype, Discord, Google Hangouts, TrueConf, MyOwnConference, Mind, GoToMeeting, VideoMost, Proficonf, то в будь-якому разі, провівши аналіз інформації стосовно реалізації та впливу кіберзагроз на вищезазначені програми телеконференцій, ще до введення в дію карантинно-обмежувальних заходів, пов'язаних з пандемією, ми побачимо реально наявні та дієві кіберзагрози в «мирний» час.

Фактично стрімко зростаюча інформатизація всіх видів діяльності конкурентоспроможних фахівців приводить до необхідності тісної взаємодії, з одного боку, у галузі інформаційних процесів і технологій, з другого боку, реалізації процесів, які мають бути підтримані засобами інформатизації. Саме на це спрямовані дії інтернет-злочинців. Протидія кіберзагрозам під час реалізації відеоконференцій нині є надзвичайно важливою проблемою. Адже під загрозу підпадає не тільки навчальний процес, одержання знань слухачами, але й практично вся господарська діяльність усієї країни.

З позиції моделювання ризиків у нашому випадку реалізується модель «небезпека – ризик», яка базується на концепції ризику як прояву (наслідку) дії небезпек різного походження. В рамках цієї моделі вважається, що результатом реалізації небезпек або породжених ними загроз є сукупність можливих негативних подій, кожна з яких характеризується парою параметрів: ймовірністю реалізації і величиною збитку, який буде отриманий у разі реалізації цієї події. Обов'язковою умовою появи ризику є наявність кількох варіантів можливого розвитку негативних подій (ризик отримання того чи іншого збитку), тобто невизначеність на рівні наслідків реалізації небезпек. Модель добре співвідноситься з механізмом утворення

DOI: 10.24025/2306-4412.3.2020.214774

ризиків для завдань захисту інформації. Відповідно до [14] було введено певну формалізацію об'єктів, безпосередньо пов'язану з існуванням ризиків, і визначено дві категорії об'єктів, з яких перша – об'єкти ризику, а друга – джерела небезпеки, тобто конкретизовано у вигляді загрози в нашому випадку. Всі загрози характеризуються своїми імовірнісними показниками, а при розгляді окремих конкретних ситуацій – відповідними збитками або втратами, гіпотетичними або реальними. Фактично наш випадок підпадає під один із базових принципів безпеки життєдіяльності – аксіоми потенційної небезпеки [14]. Суть цієї аксіоми полягає в тому, що будь-яка діяльність приховує потенційну небезпеку, тому об'єкти, які беруть участь у цій діяльності, – це об'єкти ризику, які за певних умов можуть зазнати витрат або втрат. Введені вище категорії об'єкта ризику і джерела небезпеки дають можливість описати виникнення ризиків як таких, коли у разі існування небезпеки і проявів обумовлених загроз, можливі два сценарії розвитку подій. Відповідно до першого, коли реалізація загрози (загроз) призводить до наслідків катастрофічного характеру, функціонування об'єкта ризику фактично припиняється. За другим сценарієм у результаті реалізації загроз відбувається погіршення умов функціонування об'єкта ризику. Однак в обох випадках кінцевою і принципово істотною ланкою в ряду негативних змін, викликаних впливом існуючої небезпеки, будуть втрати (витрати), яких зазнав об'єкт ризику через погіршення якості свого функціонування. За умови точного визначення властивостей небезпек (їх детермінування) існує принципова можливість обчислення фактичних характеристик вектора стану параметрів X (стан об'єкта ризику), розрахунку складових вектора Y, що являє собою цільовий комплексний показник якості об'єкта та відповідного значення скалярного показника функціонала якості (F). Якщо відхилення значень двох останніх показників від їх номінальних значень досить істотні, вживаються певні заходи щодо нейтралізації або зменшення рівня небезпек. Для цього визначаються ступінь і характер впливу кожної з небезпек на якість функціонування об'єкта ризику і згідно з результатами аналізу моделі реалізуються необхідні коригувальні дії, виконання яких нормалізує умови функціонування цього об'єкта. Тобто для цієї ситуації, коли відома вся інформація про характер небезпек, їх зв'язок зі станом об'єкта ризику і якістю його функціонування, притаманні цілком свідомі й однозначно детерміновані рішення щодо усунення небезпек або зменшення їх рівня, які гарантовано забезпечують необхідну якість функціонування об'єкта. Зауважимо, що для отримання цього кінцевого результату попередньо треба вирішити ряд завдань:

1) отримати вихідну інформацію про характер і рівень наявних небезпек;

2) визначити параметри стану об'єкта ризику (вектор X);

3) розрахувати значення комплексного цільового показника Y (або скалярного показника (F) якості роботи об'єкта ризику;

4) прийняти рішення про доцільність і, якщо це виявилося необхідним, визначити спосіб нейтралізації небезпек для нормалізації умов функціонування об'єкта ризику.

Випадок, для якого в повному обсязі досягається вирішення всіх перелічених вище завдань, насправді є ідеалізованою ситуацією, яка на практиці фактично не трапляється.

Характерною особливістю реального функціонування об'єкта ризику є наявність невизначеності при вирішенні будь-якого з перелічених вище завдань. Джерела цієї невизначеності різні. Виходячи з цього, при аналізі і вирішенні практичних завдань рівень невизначеності варіюється в досить широких межах і, як це вже було відзначено нами раніше, існують різні джерела подібної невизначеності. Зокрема, один із них – недостатня інформація про сам об'єкт ризику, його структуру, закономірності функціонування, характеристики і параметри. Тому не можна однозначно пов'язати сукупність значень складових вектора X зі значеннями елементів вектора Y, тобто відсутні точні відомості про те, як впливає стан об'єкта ризику на ефективність його роботи (на якість продукції або послуг на виході об'єкта ризику). Ця невизначеність, в першу чергу, ускладнює ефективність процедури нормалізації стану об'єкта ризику за допомогою нейтралізації небезпек, в умовах яких він функціонує.

Отже, слід підкреслити, що принциповим при аналізі та інтерпретації цієї концептуальної моделі ризиків є можливість виявлення невизначеності, породженої існуванням небезпек, яка якраз і створює ситуацію

DOI: 10.24025/2306-4412.3.2020.214774

ризиків, обумовлюючи назву моделі: «небезпека – ризик», що і проявляється в нашому випадку.

Наостанок доречно нагадати основні заходи безпеки, потрібні для захисту інформаційно-комунікативної інфраструктури в умовах дії пандемії по COVID-19 (коронавірусу):

- не клікати на лінки та не завантажувати програми, в яких ви не впевнені, щоб уникнути ризику зараження свого ПК або гаджету;

- ігнорувати онлайн-акції по вакцинації від коронавірусу і будь-яких інших, пов'язаних з вірусом пропозицій, зі значним дисконтом;

- не реагувати на листи від незнайомих адресатів з пропозицією допомогти в лікуванні вірусу і в цілому не реагувати на пропозиції, які не піддаються здоровій логіці;

- не відповідати на незнайомі номери телефону чи критично ставитися до отриманої інформації, особливо щодо вас чи ваших родичів;

- не відправляти гроші наперед при купівлі товарів в Інтернеті;

- не відчиняти двері незнайомим особам, навіть якщо вони одягнуті у спецодяг;

- перевіряти отриману інформацію в офіційних, державних і правоохоронних органах;

- проводити ретельні перевірки та background-checks по потенційних компаніях-контрагентах, постачальниках та кандидатах, у тому числі ретельно вивчаючи ціни та умови співпраці;

- в обов'язковому порядку проводити наступний (систематичний) моніторинг діючих контрагентів і постачальників з метою оперативного реагування на будь-які зміни;

- вивчати інформаційне поле навколо бізнесу, в регіонах його ведення та ситуацію в державі загалом;

- посилити фізичний і технічний захист об'єктів компанії, ключових співробітників, власників бізнесу та членів їх сімей;

- проводити періодичну перевірку ключових приміщень на технічні засоби прихованого зняття інформації;

- організувати безпечні умови праці для співробітників, клієнтів та відвідувачів під час пандемії COVID-19 (транспортування на роботу та додому, встановлення плакатів, які заохочують гігієну рук, дезінфікуючі засоби для рук, маски, рукавички, серветки, технічні засоби виявлення ознак захворювання, систематичне прибирання та провітрювання приміщень тощо);

- організувати проведення аудиту безпеки бізнесу у зв'язку зі зміною бізнес-моделі ведення фінансово-господарської діяльності, з метою оцінювання ризиків;

- розробити плани екстрених дій у випадках: масових заворушень; рейдерської атаки; нападу на об'єкти, транспорт і співробітників компанії; інформаційної атаки; неправомірних дій контролюючих та правоохоронних органів; кібератак та ін.;

- проводити періодичні онлайн-семінари зі співробітниками з питань безпеки;

- створити «Кризову групу» з метою оперативного реагування на інциденти, в яку залучити експертів з корпоративної безпеки.

Висновки. В умовах різкого розширення спектра загроз у період дії COVID-19 з'явилися нові вразливості й виникла нагальна необхідність в активізації інтересу кібергромадськості до нової проблеми, через масовий перехід населення на роботу в мережах і, отже, збільшений внаслідок цього прояв кількості та якості кібератак, а отже і збільшення кількості кіберризиків.

Аналіз літератури і джерел дослідження свідчить про недостатню увагу вчених до практичних наслідків пандемії на стан кібербезпеки і кіберризиків, які є послідовними взаємопов'язаними процедурами в процесі управління при прийнятті рішень. Генеза кіберризиків під час пандемії пов'язана з низкою технічних, психологічних, соціальних, політичних чинників, серед яких, насамперед, відзначаємо технічне навантаження на мережу та створення сприятливих умов для кіберзлочинів; збільшення використання кіберпростору пересічними користувачами, які не мають кібербезпекових навиків, психологічні аспекти пандемії сприяють неадекватному прийняттю рішень в кризовому режимі на політичному, побутовому рівнях внаслідок низького/високого рівня довіри до учасників мережі.

Оцінювання ризику передбачає дослідження стану, ситуації (сценаріїв) з наявними ознаками небезпеки, невизначеності та/або випадковості.

Найефективнішим методом уникнення цього є забезпечення юридичного підґрунтя

DOI: 10.24025/2306-4412.3.2020.214774

протидії ризикам і багатофакторне проектування або прогнозування.

На етапі оцінювання ризиків формується стратегія управління ризиками, а оскільки повністю уникнути ризиків у більшості випадків неможливо, то вагоме значення має вирішення питання допустимості (прийнятності, виправданості) ризику, яке потребує подальшого дослідження та обґрунтування.

Оцінювання ризику, що використовують у технічних системах, розглядається як процес ідентифікації інформаційних ресурсів системи та загроз цим ресурсам, а також можливих втрат, що ґрунтується на оцінюванні частоти виникнення подій і розміру збитку. Аналіз ризику розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що потребують захисту.

Перспективи подальших досліджень. Зазначені вище ризики мають принципову робочу «онлайн» складову, що дає можливість віднести їх до ризиків з великим людським фактором ризику, внаслідок якого в умовах коронавірусу користувачами робляться «вирішальні» помилки, породжені страхом і невпевненістю через багаточасове онлайн-спілкування. Саме воно, на нашу думку, сприяє появі втоми у людей і формує «швидкісні помилки» через обмеження у часі. При цьому активізується і проблема захисту персональних даних та стрімке збільшення їх крадіжок. Отже, необхідно на майбутнє проводити подальше удосконалення кібербезпеки в проявах відповідних екстремальних ризиків із урахуванням таких феноменів, як поточний стан і «конкретна» ґенеза ризику.

Список використаних джерел

[1] 2019 Internet Crime Report. FBI’s Internet Crime Complaint Center, 2020. [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf. Accessed on: Oct. 18, 2020.

[2] М. Д. Василенко, О. Б. Козін, М. О. Козіна, та В. О. Рачук, "Кіберризики в муніципальному господарстві в період пандемії: збитки та боротьба за кібербезпеку", *Комунальне господарство міст. Серія: технічні науки та архітектура*: наук.-техн. зб., вип. 3 (156), с. 80-87, Харків, 2020.

[3] В. В. Индеева, "К вопросу об определении понятия "риск". *Сборник заочных электронных конференций.* Москва: Рос. акад. естествознания, 2009. [Электронный ресурс]. Режим доступа: http:www.rae.ru/arj/ 2007/02/Indeeva.pdf

[4] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic", *Journal of Medical Internet Research*, vol. 22, no. 9, 2020. [Online]. Available: https://www.jmir.org/2020/9/e23692/pdf

[5] T. Weil, and S. Murugesan, "IT risk and resilience – cybersecurity response to COVID-19," in *IT Professional*, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330.

[6] R. O. Andrade, I. Ortiz-Garcés, and M. Cazares, "Cybersecurity attacks on Smart Home during Covid-19 pandemic," in *2020 Fourth World Conf. on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, United Kingdom, 2020, pp. 398-404, doi: 10.1109/WorldS450073.2020.9210363.

[7] Tabrez Ahmad, Corona Virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity, April 5, 2020. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3568830

[8] М. Д Василенко, "Право в теорії ризиків: ґенеза ризиків від правової до інформаційної складових (інституційний підхід)", *Юридичний вісник*, № 4, с. 43-51. Одеса: ВД «Гельветика», 2019.

[9] Б. Н. Малиновский, *Академик Виктор Глушков. Золотые вехи истории и техники Украины*. Киев, Украина: ВМУРоЛ, 2003.

[10] Международный стандарт ИСО 31000. Менеджмент риска: руководство. 2-е изд. Пер. АНО ДПО "ИСАР", 2018.

[11] P. Wagenseil, "Zoom security issues: Here's everything that's gone wrong (so far) ", *Toms Guide*, 1-3. [Online]. Available: https://www.tomsguide.com/news/zoom-security-privacy-woes. Accessed on: May 19, 2014.

[12] K. Okereafor, and O. Adebola, "Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety",

DOI: 10.24025/2306-4412.3.2020.214774

Journal Homepage, vol. 8, no. 2, 2020. [Online]. Available: http://ijmr. net. in

[13] Group-IB: шпионские программы лидируют в почтовых рассылках, паразитирующих на теме коронавируса – Group-IB Медиа-центр. [Электронный ресурс]. Режим доступа: https://www.group-ib.ru/media/covid-phishing-campaings/. Дата обращения: Окт. 18, 2020.

[14] Я. Д. Вишняков, и Н. Н. Радаев, *Общая теория рисков*: учеб. пособие. Москва, Россия: Академия, 2008.

References

[1] 2019 Internet Crime Report. FBI's Internet Crime Complaint Center, 2020. [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf. Accessed on: Oct. 18, 2020.

[2] M. D. Vasilenko, O. B. Kozin, M. A. Kozina, and V. A. Rachuk, "Cyber-risks in the municipal economy during the pandemic: losses and the fight for cybersecurity", *Komunalne hospodarstvo mist. Seriia: tekhnichni nauky ta arkhitektura*: sci.-tech. coll., iss. 3 (156), pp. 80-87, Kharkiv, 2020. [in Ukrainian].

[3] V. V. Indeeva, "To the question of the definition of the "risk" notion". *Sbornik zaochnykh elektronnykh konferentsiy*. Moscow: Ros. akad. estestvoznaniya, 2009. [Online]. Available: http:www.rae.ru/arj/2007/02/Indeeva.pdf

[4] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic", *Journal of Medical Internet Research*, vol. 22, no. 9, 2020. [Online]. Available: https://www.jmir.org/2020/9/e23692/pdf

[5] T. Weil, and S. Murugesan, "IT risk and resilience – cybersecurity response to COVID-19," in *IT Professional*, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330.

[6] R. O. Andrade, I. Ortiz-Garcés, and M. Cazares, "Cybersecurity attacks on Smart Home during Covid-19 pandemic," in *2020 Fourth World Conf. on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, United Kingdom, 2020, pp. 398-404, doi: 10.1109/WorldS450073.2020.9210363.

[7] Tabrez Ahmad, Corona Virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity, April 5, 2020. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3568830

[8] M. D. Vasilenko, "Law in the theory of risks: the genesis of risks from legal to informational components (institutional approach)", *Yurydychnyi visnyk*, no. 4, pp. 43-51. Odessa: VD "Helvetika", 2019. [in Ukrainian].

[9] B. N. Malinovsky, *Academician Viktor Glushkov. Golden milestones of history and technology of Ukraine.* Kyiv, Ukraine: VMURoL, 2003. [in Russian].

[10] International standard ISO 31000. Risk management: manual. 2nd ed. Transl. ANO DPO "ISAR", 2018. [in Russian].

[11] P. Wagenseil, "Zoom security issues: Here's everything that's gone wrong (so far)", *Toms Guide*, 1-3. [Online]. Available: https://www.tomsguide.com/news/zoom-security-privacy-woes. Accessed on: May 19, 2014.

[12] K. Okereafor, and O. Adebola, "Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety", *Journal Homepage*, vol. 8, no. 2, 2020. [Online]. Available: http://ijmr. net. in

[13] Group-IB: spyware prigrams lead the way in mailings that parasitize on the topic of coronavirus – Group-IB Media center. [Online] Available: https://www.group-ib.ru/media/covid-phishing-campaings/. Accessed on: Oct. 18, 2020.

[14] Ya. D. Vishnyakov, and N. N. Radaev, *General theory of risks*: textbook. Moscow, Russia: Academy, 2008. [in Russian].

DOI: 10.24025/2306-4412.3.2020.214774

M. D. Vasilenko, *Dr.Phys.-Math.Sc., Doctor of Law, professor,*
acting head of the Department of cybersecurity,
e-mail: nvas08@ukr.net
V. P. Novikov, *Ph.D., associate professor,*
associate professor of the Department of cybersecurity,
e-mail: novikovodessa0@gmail.com
V. O. Rachuk, *assistant of the Department of cybersecurity,*
e-mail: rachuk960@gmail.com
V. M. Slatvinska, *postgraduate student of the Department of economic law and process,*
e-mail: slatvinskaya_valeriya@ukr.net
National university «Odessa Law Academy»
Fontanskaya doroga, 23, Odessa, 65009, Ukraine

CYBERSECURITY IN THE MANIFESTATIONS OF RISKS DURING THE PANDEMIC PERIOD: CONDITION AND GENESIS

The coronavirus pandemic has created an unprecedented global emergency related to risks, including cyber-risks, which threaten cybersecurity at both local and global levels. An analysis of the information carried out by the US and EU special institutions confirms that with the appearance of COVID-19 (coronavirus) as a result of a pandemic serious risky economic and political problems are expected with a high percentage of probability. Additional problems are created by the unprecedented transition to online work, when continuous activity during a pandemic occurs mainly using remote operations.

Definitions of specific risks are contained in many standards of various sectors of the economy and equipment. However, there is an international standard ISO 31000, which is used for general risk assessment. To implement the risk management process in the current conditions in cybersecurity, it must be integrated with the components of risk management in particular and in general, including the exchange of information and consulting; establishing the context (environment); general risk assessment (its identification, analysis and evaluation); processing and summarizing the results of the selected type of risk; monitoring and critical analysis, as well as dealing with unforeseen threats.

It is shown that in the context of a fundamental increase in teleconferences (during the pandemic), the number of cyber risks significantly increases. It is noted that risks are consistent interrelated procedures that are included in the management process and require a more planned systematic approach, given that risk assessment involves studying the state, situation (scenarios) with existing signs of danger, uncertainty and/or randomness. An effective method of its implementation is to provide a legal basis and multi-factor design or forecasting. However, in the first part, the legislative decision almost always comes late. Previously, at the stage of technical risk assessment, a risk management strategy is formed, and since it is impossible to completely avoid risks in most cases, it is important to solve the issue of admissibility (acceptability, justification) of risk, which requires further research and justification. Risk assessment used in technical systems is considered as a process of identifying information resources of the system and threats to these resources, as well as possible losses, based on an assessment of the frequency of events and the amount of damage. Risk analysis is revealed as the process of identifying risks, determining their magnitude, and identifying areas that require protection.

Consequently, the COVID-19 pandemic has created and continues to create social and technical problems that are expressed in the emergence of new risks, new cyber risks. Risks become even more consistent and interconnected processes, inherently entering the management system. In this case it becomes more appropriate to make periodical checks of key premises to identify the use of technical means of hidden information retrieval and periodically conduct online seminars with security officers.

Keywords: *cybersecurity, risk, risk assessment, uncertainty, pandemic, COVID-19.*

Стаття надійшла 20.09.2020
Прийнято 18.10.2020

DOI: 10.24025/2306-4412.3.2020.214774