за разграничение ролей и доступа будет отвечать специально усиленная система безопасности Белла-ЛаПадуллы.

5. Таким образом, используя предложенный протокол безопасности, можно говорить о том, что он представляет собой основу целостной информационной технологии, работающей на основании криптографического протоколирования и сильного шифрования для обеспечения абсолютной безопасности. Данная технология может быть использована в любой сегментированной области информационной инфраструктуры, использующей высокую степень безопасности данных в транспортных слоях передачи конфиденциальных данных.

Ключові слова: криптографічний протокол, інформаційна інфраструктура, кібербезпека.
Ключевые слова: криптографический протокол, информационная инфраструктура, кибербезопасность.
Keywords: cryptographic protocol, information infrastructure, cybersecurity.

Василенко Микола Дмитрович
Національний університет «Одеська юридична академія»
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

Новіков Вячеслав Пантелійович
Національний університет «Одеська юридична академія»
доцент кафедри кібербезпеки, к.т.н, доцент

Рачук Валерій Олександрович
Національний університет «Одеська юридична академія»
асистент кафедри кібербезпеки

БЕЗПЕКА ТА ВИКЛИКИ СУЧАСНОСТІ: РИЗИКИ ТА КІБЕРБЕЗПЕКА В ПЕРІОД ПАНДЕМІЇ

Інформація, яка надходить з різних країн світу свідчить про те, що в результаті пандемії з великим процентом ймовірності очікуються ризикові економічні та політичні негаразди.

З появою коронавірусу (COVID-19) додаткові проблеми з'явилися майже у всіх країнах і в усіх владних структурах, а урядові рекомендації, що стосувалися COVID-19, призвели до безпрецедентного переходу співробітників на дистанційний режим роботи.

Все це разом з різким скороченням персоналу і фінансовою кризою викликали стрімке зростання комп'ютерної злочинності. Так, аналітиками компанії Group-IB, міжнародної компанії, основним напрямком діяльності якої є розробка методів і засобів запобігання кіберзагроз в реальному часовому масштабі, позначені основні тенденції комп'ютерних злочинів в період пандемії COVID-19, на тлі різкого збільшення зростання числа кіберзагроз. Наприклад, в одному з основних напрямків комп'ютерної злочинності, на перший план висуваються методи фінансових шахрайств на базі соціальної інженерії при надзвичайно активній експлуатації теми COVID-19. Зараз це проявляється найчастіше в різкому збільшенні шкідливих розсилок, перемиканні операторів вірусів-шифрувальників на найширшу тематику і більш вишукану цільову вибірковість, а також активний рекрутинг в злочинні спільноти нових учасників.

Однією з головних поточних тенденцій цифрової трансформації сучасного періоду провідні світові аналітики одностайно називають розвиток дистанційних способів вчинення злочинів, при яких відсутній фізичний контакт між зловмисниками та їх жертвами – злочини пішли з офлайну в онлайн. Такі трансформації неминуче призводять до різкого збільшення числа кіберризиків, і зокрема, до зростання всіляких інших ризиків в середовищі простих користувачів ПЕОМ.

Проте також важливим залишається проведення необхідних заходів для забезпечення зниження ризиків в цілому, і кіберризиків зокрема, в цих виняткових обставинах. Через те, під час пандемії безперервна діяльність, в основному, відбувається завдяки використанню віддалених операцій, у світі з'явилась величезна кількість «фішингових» кампаній. Загальновідомо,

що фішинг являє собою « різновид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів » [1]. 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 міститься пряме посилання на сайт, зовні невідмітний від сьогодення, або на сайт з редиректом. Після того, як користувач потрапляє на підробну 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 дозволяє шахраям отримати доступ до облікових записів та банківських рахунків. У той час як сьогодні в багатьох країнах запроваджувалися заходи, щоб допомогти жертвам COVID-19 і обмежити зараження, хакери використовують кризу і продовжують свої дії для здійснення цілеспрямованих кібератак на підприємства, зокрема, на робочі місця. У період кризи хакери намагаються використовувати увагу, яку приділяють вірусам, і зв'язаними з ними панічно ефекту для проведення фішингових кампаній, видаючи себе за оповіщення, що зв'язані з COVID-19 (див. [1]). Отже, майже всі випадки можливих загроз базуються на розумінні та використанні ризиків та ризикових ситуацій. Водночас в умовах необхідності створення безпеки в інформаційно-комунікаційних системах, оцінка та якісний аналіз інформаційних ризиків дозволяє 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. Оцінка 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'язаними з нею поняттями. В цьому випадку можливий вимір результату визначається ймовірністю матеріальних та інших втрат через вірогідність появи несприятливого результату або події. Зустрічається 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'язаного з нею шкоди. Зустрічаються і визначення ризику, які відображають його як небезпеку вибору з двох або більше альтернативних варіантів дій та передбачає 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, не сприятливої); поняття ризику розкривається через практичну діяльність суб'єкта; ризик розкривається через незалежну від суб'єкта діяльності подію, наступ якої, кількісно можливо оцінити; при цьому, часто акцент робиться на кількісну та якісну оцінку ризику – «міру 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 (декотрої сумарної величини). В цьому разі при обговоренні поняття «ризику», можна виділити одну характеристику, яка зустрічається у всіх 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. Пов'язані з коронавірусною пандемією карантинні заходи і режими самоізоляції

призвели до різкого зростання різних онлайн-сервісів – в це число входять в 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 призвів до проявів нових вразливостей. Результатом чого було різке зростання кіберзлочинів, що корелює із зростанням попиту на онлайн-сервіси. 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 вищевказані програми телеконференцій, ще до введення в дію карантинно-обмежувальних заходів, пов'язаних з пандемією, ми побачимо реально наявні та дієві кіберзагрози в «мирний» час. Отже, ризики стали послідовними взаємопов'язаними процедурами, які входять у процес управління, а оцінка ризику передбачає дослідження стану, ситуації (сценаріїв) з наявними ознаками небезпеки, невизначеності та/або випадковості. Найефективнішим методом її здійснення є забезпечення юридичного підґрунтя та багатофакторне проєктування або прогнозування. На етапі оцінки 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. Оцінка ризику, що використовують в технічних системах, розглядається як процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів, а також можливих втрат, заснований на оцінці частоти виникнення подій і розмір збитку. Аналіз ризику

розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що вимагають захисту. Таким чином, зазначені вище ризики мають принципову робочу «онлайн» складову, що дозволяє 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 та формує «швидкісні помилки» через обмеження у часі. Активізується при цьому і проблема захисту персональних даних та стрімке збільшення їх крадіжок. Отже, необхідно на майбутнє проводити подальше удосконалення кібербезпеки, що спотворить умови протистояння найбільш вагомим викликам сучасності – пандемії в прояві COVID-19.

Список використаних джерел:

1. Василенко М. Д., Козін О. Б., Козіна М. О., Рачук В. О. Кіберризики в муніципальному господарстві в період пандемії: збитки та боротьба за кібербезпеку. Науково-технічний збірник «Комунальне господарство міст». Серія: технічні науки та архітектура. Харків, 2020. Т. 3. Вип. 156. С. 80–87.

Ключові слова: ризик, кібербезпека, «онлайн», невизначеність, оцінка, пандемія, COVID-19.

Ключевые слова: риск, кибербезопасность, «онлайн», неопределенность, оценка, пандемия, COVID-19.

Keywords: risk, cybersecurity, «online», uncertainty, assessment, pandemic, COVID-19.