3. Опанасенко Е. Конференции в Zoom оказались под угрозой: хакеры воруют пароли [Електронний ресурс] – Режим доступу до ресурсу: https://www.segodnya.ua/lifestyle/science/konferencii-v-zoom-okazalis-pod-ugrozoy-hakery-voruyut-paroli-1425732.html. – Назва з екрана. – Дата перегляду: 10.04.2020.

Ключові слова: конфіденційна інформація, відеоконференція, інформаційна безпека, шифрування.
Ключевые слова: конфиденциальная информация, видеоконференция, информационная безопасность, шифрование.
Key words: confidential information, video conferencing, information security, encryption.

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

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

КОЗІН ОЛЕКСАНДР БОРИСОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки,
кандидат фізико-математичних наук, доцент

ПАПКОВСЬКА ОЛЬГА БОРИСІВНА

Одеський національний політехнічний університет,
доцент кафедри вищої математики та моделювання систем,
кандидат фізико-математичних наук, доцент

РИЗИКИ: ПРАВОВА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Із багатьох публікацій у вітчизняних та іноземних виданнях відомо безліч визначень ризику, що несуть досить широке його тлумачення. Так, тільки у Інтернет-словниках міститься сотні тлумачень ризику у багатьох сферах людської діяльності (див. [1]). В наслідок цього виникають різні неоднозначності, пов'язані з розкриттям сутності самого ризику та пов'язаних з ним понять. Це стосується як технічної, так і юридичної сфери. Ризик має досить широке трактування. При цьому його соціальна сутність полягає перш за все в тому, що суб'єкт, свідомо відступаючи від встановлених в суспільстві правил поведінки, створює конфліктну ситуацію, загострює до межі проблему і, використовуючи переваги екстремальної ситуації, намагається вирішити поставлене завдання. Тому зрозумілим стають ймовірні ризики від непрофесійних керівників, які вважають себе «ефективними менеджерами». Відповідно такий стан характерний також і для сфери інформаційної безпеки та кібернетики, яка в даний час впроваджена в будь-яку систему управління. В 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 зачіпають різні предметні галузі, то це поняття слід розглянути з точки зору безпеки, психології, економіки, страхування, медицини, геології тощо. Воно відображене як в безлічі публікацій, так і в різних нормативних документах (див., наприклад, [1]). Втім, виникає проблема управління різними видами ризиків, що потребує, на наш погляд, інституційного розуміння. Крім того, для розв'язання, наприклад, управлінських задач слід визначитися з використання прогнозування (оцінки) ризиків. Нерідко для цього автори виходять з позицій кібернетичного бачення явища і кібернетики в цілому, яка, за визначенням академіка В.М. Глушкова, представляє собою науку про загальні закони одержання, зберігання, передавання й перетворення інформації у складних системах управління [2].

Визначення ризику містяться в багатьох нормах різних галузей права (міжнародного, господарського, фінансового тощо). У нормах приватного права (цивільного, страхового, фінансового тощо) інститут ризику служить підставою для попереджуючого перерозподілу збитків. В той же час існує Міжнародний стандарт ISO 31000 [3], 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; установлення контексту (оточення); загальне оцінювання ризику (його ідентифікація, аналіз та оцінювання); оброблення ризику; моніторинг і критичне аналізування.

Міжнародний стандарт ISO 31000 враховує, в цілому, більшу частину можливих ризиків та пов'язаних з ними складових, в тому числі й юридичних ризиків. Щодо юридичних ризиків зауважимо, що враховуючи єдність регулятивних і охоронних правовідносин (коли, наприклад, кримінальні закони охороняють інтереси, що регламентують адміністративне, цивільне право), в одному процесі правозастосування юрисдикційний орган стикається з інститутом, в якому існують протилежності, які формують інститут ризиків і балансуються все ж таки судовою практикою. З позиції загальної теорії ризиків слід звернути увагу на принципову особливість, а саме на те, що «прогнозуванням» часто замінюють «оцінку» ризиків. Прогнозування використовують в нетехнічній сфері, і тут воно, схоже, функціонує аналогічно оцінці. Однак між ними існує різка відмінність у стандартній моделі статистичної проблеми. Однак в юридичній галузі 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 необхідності 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. Небезпека в даному випадку може і не загрожувати. При крайній необхідності порівнянню підлягає тяжкість шкоди заподіяної і такої, що

запобіг, а при ризику акцент робиться на порівняння ступеня вірогідності спричинення шкоди (наприклад, допустимий ризик тяжких наслідків, але з мінімальним ступенем вірогідності).

В інформаційних технологіях ризики мають суттєве значення та визначаються вираженою конкретикою. В умовах необхідності створення інформаційної безпеки оцінка інформаційних ризиків дозволяє визначити необхідний рівень захисту інформації та здійснити його. Оцінка інформаційних ризиків дозволяє визначити необхідний рівень захисту інформації, здійснити його підтримку і розробити стратегію розвитку інформаційної структури компанії. Оцінка та аналіз інформаційних ризиків є необхідною умовою при створенні системи управління ризиками і плану забезпечення безперервності і відновлення бізнесу. У разі дослідження інформаційної безпеки ризик часто відображається імовірністю або пов'язаними з нею поняттями (вимірювана ймовірність втрат, поява несприятливого результату або події). Також зустрічається 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 і розміри пов'язаного з нею шкоди. Зустрічаються і визначення ризику, які відображають його як небезпеку вибору з двох або більше варіантів дій та передбачає хоча б мінімальне збереження вже досягнутого, з іншого.

При дослідженні технічних ризиків, виділяють їх базові витоки: ризик розглядається як вимірювана або розрахована ймовірність; ризик пов'язують з настанням певної події (як правило, не сприятливої); поняття ризику розкривається через діяльність суб'єкта; ризик розкривається через незалежну від суб'єкта діяльності подію; акцент робиться на кількісну та якісну оцінку ризику – «міру ризику»; поняття ризику розкривається через невизначеність; ризик відображається ситуацією вибору з двох або з п варіантів дії; ризик сприймається як небезпека, частота, витрати і втрати, характеристика ситуації, сумарна величина. В цьому разі при обговоренні поняття ризику, можна виділити одну характеристику, яка зустрічається у всіх визначеннях, наведених вище, та об'єднує їх. Це подія, яка має відбутися і яка пов'язана з імовірністю, дією або діяльністю, мірою, частотою, вибором певних рішень, невизначеністю, з втратами, небезпекою і т.д. При цьому саме управління ризиками розглядають як процес ідентифікації, управління, усунення або зменшення ймовірності подій, здатних негативно впливати на ресурси інформаційної системи, зменшення ризиків безпеки, потенційно мають можливість впливати також на інформаційну безпеку, за умови прийнятної вартості засобів захисту. Управління ризиками включає в себе всі операції, які можна проводити над ризиком інформаційної безпеки: мінімізація, нейтралізація, прийняття ризику, передача ризику або страхування.

Аналіз та оцінка ризику визначають послідовними взаємопов'язаними процедурами, які входять у процес управління. Оцінка ризику 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. Отже, прийняття раціональніших рішень у цих випадках вимагає використання специфічного математичного апарату теорії ігор. Цільова невизначеність виникає у багатоцільових завданнях, які потребують багатокритеріального вибору оптимальних рішень.

Таким чином, ризики є 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 проектування 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.

Список використаної літератури:

1. Индеева В.В. К вопросу об определении понятия «риск». Сб. заочных электронных конференций. Электрон. дан. – М.: Российская Академия Естествознания. 2009. [Електронний ресурс] – Режим доступу до ресурсу: URL:http:www.rae.ru/arj/2007/02/Indeeva.pdf
2. Малиновский Б.Н. Академик Виктор Глушков. Золотые вехи истории и техники Украины. К.: ВМУРоЛ. 2003. – 183 с.
3. ИСО 31000:2018 Менеджмент риска. Руководствою 2-е изд. Международный стандарт/ Перевод АНО ДПО «ИСАР». – 2018. – 19 с.

Ключові слова: ризик, оцінка ризику, управління ризиком, невизначеність, правові ризики, інформаційні ризики.

Ключевые слова: риск, оценка риска, управление риском, неопределенность, правовые риски, информационные риски.

Key words: risk, risk assessment, risk management, uncertainty, legal risk, information risk.