

якій треба чітко спланувати розвиток інформаційної безпеки, удосконалити політику безпеки в цій галузі, визначити ризики і загрози інформаційній безпеці, джерела цих загроз, способи та методи їх реалізації. А також удосконалити засоби захисту, що вже існують, і розробити нові, з метою впровадження, експлуатації та розподілу адміністративних інформаційних ресурсів.

Список використаних джерел:

1. Соломко Ю. . Електронне урядування: поняття, сутність, принципи та напрями розвитку. Ефективність державного управління, 2018, ВИП. 2 (55), Ч. 1.
2. Концепція розвитку електронного урядування в Україні: Розпорядження КМУ від 20.09.2017 № 649-р.

Ключові слова: інформаційна безпека, електронне урядування, адміністративні інформаційні ресурси, загрози інформації

Ключевые слова: информационная безопасность, электронное управление, административные информационные ресурсы, угрозы информации

Keywords: information security, e-governance, administrative information resources, information threats

Василенко Микола Дмитрович

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

Матковська Інга Олексіївна

студентка 4 курсу факультету кібербезпеки
та інформаційних технологій

ДЕЯКІ ПИТАННЯ РИЗИКІВ (ІНФОРМАЦІЙНИХ РИЗИКІВ) В КОНТЕКСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Відомо, що соціальна інженерія сформувалася в науку і представляє собою вивчення людської поведінки та факторів,

які на неї впливають. Вона досліджує причини поведінки тої чи іншої людини та обставин та середовища, що впливають на формування системи її цінностей та саму поведінку [1]. Оскільки на чолі приведенного визначення стоїть людина та її поведінка, то важливою стає створена нею безпечна ситуація, яка проявляється, в першу чергу, в ризиках, пов'язаних з діяльністю самою людиною. Відбувається проникнення ризику в усі сфери людської діяльності, а тому поділяти ризики на види досить важко: це процес нескінченний і недоцільний. Однак доречним сталося дослідити ризики за механізмом виникнення. Так, виділяють ризики, пов'язані з несприятливими умовами життєдіяльності (функціонування організацій); ризики, зумовлені небезпечними явищами (форс-мажором) в природному, техногенному, соціальному та діловому середовищі; зумовлені негативними тенденціями розвитку, що приводять до криз (для організації до погіршення її фінансового стану і в результаті до банкрутства). Тенденції можуть бути пов'язані із зовнішніми факторами, що формують несприятливу кон'юнктуру для організації, або з внутрішніми, пов'язаними, наприклад, з протиріччями всередині самої організації [2].

В зазначених вище умовах виникає ситуація невизначеності, яка представляє собою сукупність обставин і умов, за яких можливі зміни стану об'єкта ризику стають абсолютно непередбачуваними. Ця ситуація виключає можливість об'єктивного оцінювання ризику. Однак певне зменшення невизначеності порівнята з такою статистичною невизначеності породжує ризикову ситуацію, яка характеризується існуванням кількох можливих станів (як варіант – множини станів, що сягає нескінченості), ймовірність реалізації кожного з яких відома. Якщо реалізацію на об'єкт ризику будь-якого з можливих станів вважати подією, РС визначається існуванням множини варіантів можливого розвитку подій, ймовірність кожного з яких характеризується відповідною кількісною або якісною оцінкою. За умов виникнення ризикової ситуації стає

актуальним проведення аналізу й оцінювання ризиків, зокрема дослідження обставин появи, умов та форм розвинення ризиків.

Отже, загалом під невизначеністю розуміють неповне або неточне уявлення про значення різних параметрів в майбутньому, що породжується неповнотою і (або) неточністю інформації щодо виникнення в ході реалізації рішення несприятливих ситуацій і наслідків, що призводить до ризику. У той же час ситуація ризику вважається фактично різновидом невизначеності, коли при настанні подій ймовірно і об'єктивно існує можливість оцінити їх вірогідність. Різниця між ризиком і невизначеністю відноситься до способу завдання інформації та визначається наявністю (у разі ризику) або відсутністю (при невизначеності) імовірнісних характеристик неконтрольованих змінних. Ці відмінності враховуються в математичній теорії дослідження операцій, де розрізняють задачі прийняття рішень при ризикі і відповідно в умовах невизначеності.

Інформаційна невизначеність є або єдиною основою випадковості події для людини, або вона супроводжує і доповнює об'єктивну випадковість. З такого висновку виходить інформаційна парадигма ризиків будь-якої природи: інформаційна невизначеність є суть усіх ризиків. При таких умовах важливим чинником в ризиках стає психологічна складова явища. При цьому будь-яке прийняття рішення ґрунтується на мисленні, що відбувається в умовах невизначеності (в більшій чи меншій мірі), на особистісній зумовленості виборів і особистих або соціальних моделях прийняття рішення. Незалежно від інтелектуальної бази мислення конкретної людини, специфіки техногенної або соціальної ситуації, в якій він змушений діяти, особливості морально-етичних, моральних установок, ступеня інтенсивності їх відстоювання індивідом всі варіанти прийняття ризикованого рішення об'єднує загальна властивість – вони є реалізацією суб'єктом інтелектуально-особистісних зусиль, спрямованих

на зниження рівня невизначеності ситуації. При цьому людина сприймає своє рішення як довільний вибір, здійснений ним відносно вільно (асpekt вимушеність присутній завжди, але не завжди пригнічує волю) в рамках певної альтернативи можливих варіантів поведінки. Інформаційна складова ризику найбільш вагома у випадках використання прогнозової інформації, дефіциту часу на обробку інформації і ухвалення рішення, в умовах активної інформаційної протидії конкурентів або супротивника. На відміну від інших складових ризику інформаційна складова обов'язково є присутньою в кожній ризиковій події. Змінюється лише її відносна величина.

Настанню ризикової події можуть сприяти свідомі або неумисні дії людини. Навіть маючи якісну інформацію, фахівець може прийняти неправильне рішення або виконати неприпустиму дію, яка спричинить реалізацію ризикової події. Значна частина ризикових подій пов'язана з технічними системами, технологічними процесами, отриманими людиною речовинами і іншими об'єктами, що є продуктами людської діяльності. Техногенні аварії, збої і відмови устаткування, екологічні катастрофи, пандемії далеко не вичерпують повного переліку компонентів цього типу. Людина майже безсила перед цілим рядом стихійних лих. Значна частина з них доки ще не піддається точному і своєчасному прогнозуванню.

Сьогодні практично відсутні дієві підходи до трактування поняття «Інформаційний ризик», в яких в якості можливих небажаних подій розглядалися б події, що призводять до зниження достовірності, повноти та актуальності інформації на стадії її отримання та введення в інформаційну систему. У поняття інформаційний ризик не включають також ризики, пов'язані з можливою наявністю помилок в моделях, алгоритмах обробки інформації, програмах, які використовуються для вироблення рішень, що управляють, і виготовленні безпосередньо з участю людини. Разом з технічною складовою і в інформаційних ризиках основною все ж-таки залишається людина. Виникають складності у розпізнаванні достовірної (недостовірної)

вірної) інформації: треба враховувати морально-етичний стан людини, а також стан правового регулювання, захисту персональної інформації особи та постійне технічне удосконалення конкретних інформаційно-комунікаційних систем [1].

Достатньо швидко технічні системи захисту все більше й більше удосконалюються за рахунок постійного розвитку сучасних технологій, обліку безлічі потреб, які створюють додаткові ризики. До грамотно відбудованим технічним системам захисту можна тривалий час не підходити і останні будуть справно виконувати свої основні функції та завдання, а люди як і раніше будуть

залишатися найбільш вразливою ланкою, коли вони мають доступ до інформації та на них можна впливати методами соціальної інженерії.

Соціальні інженери користуються тим, що психологічні маніпуляції не вимагають великих витрат і специфічних знань (крім кількох психологічних прийомів), їх можна застосовувати протягом тривалого часу, а ще їх складно виявити. Люди, які володіють цінною інформацією або мають до неї доступ, можна порівняти з доступним плодом: вони на увазі і до них дуже легко дотягнутися.

Захищатися від технік соціальної інженерії складно, так як жертви часто не здогадуються про те, що їх обдурили і використали їх слабкості, щоб роздобути конфіденційну інформацію. Вирішити проблему можна одним способом: підвищувати нашу усвідомленість. А для цього нам доведеться навчитися правилам роботи з інформацією і донести небезпеку її розкриття, щоб вміти визначити інформацію, вразливу до атаки [3].

Тему ризиків в контексті соціальної інженерії можна можна продовжувати і далі, але це все одно не захистить інформаційні технології і апаратуру від зловмисників і шахраїв усіх мастей. Впливає один вахливий висновок: типових протидій діям соціальних інженерів і соціальній інженерії не існує і, напевно, чи може існувати. Кожна ситуація вимагає індивідуального підходу і всебічного розгляду.

Список використаних джерел:

1. Резник Ю. М. Соціальна інженерія: предметна область і межі застосування. Социс. 1994. № 2. С. 28–34.
2. Василенко М. Д., Козін О. Б. Право в теорії ризиків: генеза ризиків від правової до інформаційної складових (інституційний підхід). Юридичний вісник. – О.: ВД «Гельветика». 2019. № 4. С. 43–51.
3. Касперски Кріс. Секретна зброя соціальної інженерії: Компанія АйТи. 2005. С. 15.

Ключові слова: соціальна інженерія, людина, ризики, інформаційні ризики, невизначеність, метод, інформаційні атаки.

Ключевые слова: социальная инженерия, человек, риски, информационные риски, неопределенность, метод, информационные атаки.

Keywords: social engineering, human, risks, information risks, uncertainty, method, information attacks.

Трофименко Олена Григорівна

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

АНАЛІЗ СТАНУ Е-УРЯДУВАННЯ В УКРАЇНІ

За умов повсюдного дистанціонування та карантину, спричинених глобальним спалахом пандемії COVID-19, цифрові рішення стали життєво важливими для подолання ізоляції, інформування та спілкування людей. Уряди усього світу докладають наполегливих цифрових зусиль щодо залучення нових способів надання якісних е-послуг.

Світовий досвід доводить, що е-урядування надає значні можливості для трансформації системи державного управління в інструмент сталого розвитку разом зі зменшенням часових і матеріальних витрат громадян і бізнесу при взаємодії з державою, забезпеченням прозорості діяльності органів влади, суттєвим зменшенням бюрократії і корупції, залученням громадян до участі у державних справах [1].