Облог С. В., Зборовська Т. В.

Національний фармацевтичний університет, м. Харків

Оцінка інформаційних ризиків як запорука конкурентоспроможності та якісного управління

34444@i.ua

Вступ. Інформація – це дуже вагоме та змістовне слово. «Хто володіє інформацією, той володіє світом» – відомий вислів Натана Ротшильда, пізніше процитований і поширений Вінстоном Черчиллем, сьогодні актуальний як ніколи.

У сучасному світі інформаційних технологій ставлення до інформації дуже різноманітне, та суперечливе. Інформація може бути загальнодоступною, та закритою, вона може бути захищеною, та, у той же час, відкритою для загалу, змінною або недостовірною, тощо. Кожна компанія, від маленького підприємства до великих корпорацій має власне ставлення до інформації. Всі хочуть отримати якомога більше інформації стосовно ринків збуту продукції, виробництва, фінансової інформації, даних про конкурентів та партнерів, у той же час зберегти в таємниці свою комерційну інформацію, втрата, або розповсюдження якої може фатально вплинути на діяльність компанії та її позицій на ринку.

Основні ризики, які можуть бути розглянуті щодо інформації підприємства, пов’язані з неправильним підходом до керування інцидентами інформаційної безпеки; незахищеністю активів IT-інфраструктури; неналежним захистом інформації у мережах та на носіях з використанням технічних уразливостей цих самих носіїв, тощо.

Аналіз стандартів з інформаційної безпеки дозволяє виявити основні елементи ризиків, які описуються інформаційною структурою та визначають вплив на діяльність інформаційних систем. Під ризиком розуміють можливість або ймовірність настання подій з негативними або позитивними наслідками в результаті певних рішень або дій. Тому потрібно проводити оцінку ризику –

процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів, а також можливих втрат, заснований на оцінці частоти виникнення подій та розміру збитку від них.

Мета дослідження. Виходячи з цього ми ставимо за мету нашої роботи провести дослідження щодо встановлення методичних підходів з оцінки різного роду впливів, наприклад таких ризиків як втрата або несанкціоноване розповсюдження комерційної інформації, та їх наслідків і заходів з протидії на успішність функціонування підприємства.

Матеріали та методи. В наших дослідженнях в якості матеріалів ми використовували аналіз джерел літератури, вимог стандарту ISO/IEC 27001:2022 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» та досвіду провідних підприємств різних галузей, які впровадили інформаційний захист у вигляді сертифікації системи управління інформаційної безпеки.

Результати дослідження.

Проаналізувавши вимоги стандарту можемо встановити етапи управління інформаційною безпекою підприємства наведені на Рис.1:

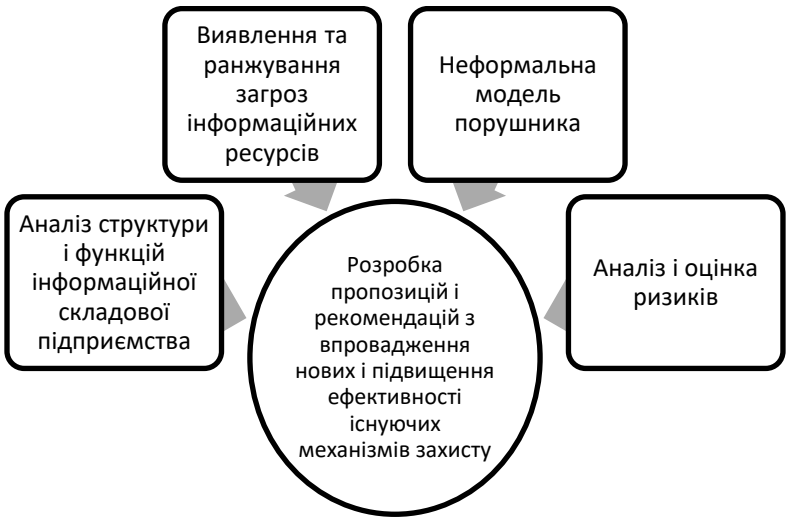

Рис.1. Сценарій управління інформаційною безпекою підприємства.

Які найчастіше виникають ризики щодо втрати або розповсюдження комерційної або закритої інформації? Наприклад, втрата інформації найчастіше виникає при поломці або відмові обладнання, при втраті живлення, або при

помилкових діях персоналу та користувачів обладнання. Також ризик втрати даних буває мнеш передбачуваним – це, наприклад, може бути навмисне або випадкове зараження комп'ютерних систем шкідливими програмами. Іншими ризиками для компаній може бути витік або розповсюдження комерційної інформації. Цей тип ризиків також є менш передбачуваним, але дуже впливовим. Ризики, пов'язані з розповсюдженням інформації можуть зашкодити розвитку компанії, або діяльності в цілому, що у свою чергу може привести до втрати конкурентних позицій та відтоку клієнтів.

Ризики інформаційної безпеки є складовою частиною операційних ризиків підприємства. Одним із шляхів вирішення проблеми оцінки ризиків та вибору оптимального варіанта їх обробки є визначення методики з отриманням необхідної інформації для проведення оцінки з метою прийняття обґрунтованих рішень стосовно того, яким чином краще забезпечувати захист активів підприємства від певних загроз інформаційної безпеки. Оцінка ризиків інформаційної безпеки може здійснюватися у розрізі підприємства або його інформаційних систем.

Оцінка ризиків інформаційної безпеки складається з етапів припустимого та існуючого ризику здійснення загрози, значення ймовірності кожного із загроз допомагає співвіднести оцінку можливих збитків із витратами на захист.

Таблиця 1.

Етапи ризик-орієнтованого підходу в інформаційній безпеці підприємства

Етап роботи з інформаційними ризиками	Необхідні дії з боку підприємства
Ідентифікація загроз відповідно до специфіки діяльності	Формування повної множини загроз для інформаційних потоків
Ідентифікація джерел та каналів інформаційної діяльності	Визначення переліку об'єктів інформації, що потребують захисту
Ідентифікація джерел загроз	Виявлення можливих джерел впливу (ризиків) на інформаційні потоки
Ранжування інформаційних ризиків за ступенем впливу та ймовірністю настання	Аналіз і вибір переліку ризиків, з огляду на особливості функціонування підприємства та оцінка наслідків їх впливу, визначення імовірності здійснення потенційних загроз
Оцінка наслідків	Обрахунок можливого рівня фінансових, технологічних та іміджевих втрат
Корегування інформаційного захисту	Розробка заходів з попередження та коригування наслідків інформаційних загроз

Отже ризики ми можемо класифікувати за властивостями інформаційних ресурсів, які порушуються при розвитку кризової ситуації (цілісність, доступність, конфіденційність), а також ризики за втратами, в наслідок настання кризової ситуації. Втрати можуть бути по-перше фінансовими, далі – репутаційними, (порушення контрактів), порушення законодавства. З наведених типів втрат, фінансові втрати найбільше піддаються кількісній оцінці. Репутаційні втрати частково можливо оцінити з фінансової точки зору – це, наприклад, втрата контрактів, яка призведе до фінансових втрат компанії, та до втрати її конкурентоспроможності.

При визначені ступеню потенційної загрози, підприємства повинні проводити оцінку ризиків, за впровадженою програмою ризик-менеджменту. Оцінка ризиків, в свою чергу, допоможе впровадити відповідні заходи для зниження або усунення ризиків.

Висновки. Для визначення та передбачення несприятливих подій, загрози треба проаналізувати заздалегідь в поєднанні з потенційними вразливостями. Також повинні бути проаналізовані потенційні місця прояву цих несприятливих подій. Рівень впливу тієї чи іншої ризикової ситуації визначається величиною збитку, який може бути заподіяний відповідними загрозами. Такий підхід дає можливість, у подальшому, сформувати рекомендації щодо формування програми ризик-менеджменту ІТ-інфраструктури підприємства.