УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА ДЛЯ УТРИМАННЯ КОНКУРЕНТНИХ ПОЗИЦІЙ НА РИНКУ

Д. М. Такій, *магістр,*
О. А. Журан, *к.е.н., доцент*
Одеський національний політехнічний університет

Актуальність. Поняття «інформаційна безпека» з'явилось завдяки розвитку засобів інформаційних комунікацій серед суспільства. У сучасному світі стрімкий розвиток інформаційних технологій не є новиною. Збільшується кількість інформаційних систем, програмних забезпечень , які допомагають персоналу підприємства управляти інформаційними потоками. Відповідно до цього збільшується кількість цінної інформації. Тому питання про її захист стоїть досить гостро.

Аналіз останніх досліджень і публікацій. Аналізу захисту інформації підприємства присвячені роботи таких авторів: Шевченко С. Ю., Нашинець-Наумова А. Ю., Чунарьова А. В., Чунарьов А. В., Герасименко А. В., Козак А. В..

Метою роботи є розгляд проблемних питань по управлінню інформаційною безпекою підприємства для забезпечення конкурентоспроможності.

Основний матеріал. Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття інформаційна безпека».

Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення[1].

Мета інформаційної безпеки полягає в тому, щоб зберегти цілісність, повноту та точність інформації, зменшити ризик несанкціонованих змін у інформаційних системах.

Захист інформації на підприємстві є важливим завданням, що може впливати на фінансову та виробничу його діяльність і як наслідок на ринок, в якому існує. Для того, щоб забезпечити підприємству розвиток та конкурентоспроможність, необхідно створити систему управління інформаційною безпекою.

У інформаційну безпеку підприємства входить сукупність напрямів, методів, засобів і заходів, що знижують незахищеність інформації і не дають можливість зловмисникам доступу до інформації, її розповсюдженню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи[2].

Варто наголосити, що головним напрямом у процесі забезпечення інформаційної безпеки підприємства являється утримання у таємниці комерційної інформації, що дозволяє підприємству успішно залищатися конкурентоспроможним на ринку товарів та послуг.

Якщо конфіденційність, цілісність, доступність, достовірність тощо знаходяться в критичному стані, то це може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення достовірності персональних даних фізичних осіб.

Наслідком вище сказаного може стати: проблеми у ділових справах; зриви переговорів з конкурентами, втрата вигідних контрактів; невиконання договірних зобов'язань тощо.

Для розв'язання проблем інформаційної безпеки підприємства необхідно створити підрозділ інформаційної безпеки, який входить до складу служби економічної безпеки підприємства. Даний підрозділ повинен підкорятися вищому керівництву. Загалом до таких підрозділів входять такі фахівці як системні адміністратори.

Для того, щоб організація функціонувала ефективно, необхідно ідентифікувати та управляти багатьма процесами, а саме управляти ризиками інформаційного об'єкту. Для того, щоб поєднати економічну ефективність з прийнятим рівнем ризику, а необхідно організувати процес управління ризиками. Це зрозумілий метод для організації власних інформаційних ресурсів з обмеженим доступом для керівників різних рівнів. Якщо такий процес почне діяти на підприємстві, то це дозволить знизити рівень ризика з критичного до допустимого. Проте для кожної організації необхідно створювати різні моделі управління інформаційною безпекою, універсальної моделі не існує, адже необхідно враховувати специфіку. В залежності від структури певної інформаційної системи визначається допустимий ризик та підхід до управління інформаційною безпекою. Усі моделі різні, вони можуть включати свої ресурси, час, складність та суб'єктивність. Правильно створена програма та методи управління ризиками дозволить дотримуватися діючих законодавчих вимог та створить необхідний рівень захищеності інформаційних ресурсів підприємства. На початковому етапі необхідно оцінити ризики організації перед розробкою та експлуатацією інформаційних систем. Через оцінки ризиків ідентифікуються загрози активам, оцінюються їх уразливість й імовірність виникнення загроз, а також можливий руйнівний вплив під час реалізації несанкціонованих дій. Далі запропоновано сценарій управління ризиками інформаційного об'єкту[3].

Запропонований сценарій розрахунку ризиків складається з наступних базових складових, а саме:

– визначення методології оцінювання ризику для інформаційної системи;

– розроблення критеріїв ухвалення ризиків та визначати прийнятні рівні ризику;

– визначення активів;

– виявлення небезпеки для активів;

– виявлення вразливих місць в системі захисту;

– виявлення дій, які порушують конфіденційність, цілісність та доступність активів;

– визначення ймовірність провалу системи безпеки за наявності переважних небезпек та вразливостей;

– оцінка рівнів ризику;

– визначення прийнятності ризику або ж вимагати його скорочення, використовуючи встановлені критерії допустимості ризику;

– вибір завдань та засобів управління для скорочення ризиків (завдання та засоби управління мають бути вибрані та упроваджені відповідно до вимог, встановлених процесом оцінки ризиків та скорочення ризиків. Цей вибір повинен враховувати як критерії допустимості ризику, так та юридичні, регулятивні та договірні вимоги) [3].

Висновки

Збереження інформації – це те питання, яке заслуговує уваги, адже хто володіє інформацією, той володіє світом. Тому важливо слідкувати за потоками отриманої інформації, за її цілісністю, правдивістю та актуальністю. У наш час існує безліч інформаційних технологій, які дозволять зробити цей процес швидшим та зручнішим, проте необхідно пам'ятати, що останнє рішення завжди залишається за людиною, за керуючою особою. Якщо на підприємстві ведеться постійний моніторинг за ринком, за конкурентами, то це дозволить йому стати конкурентоспроможним, розробляти нові технології та продукцію, йти в одну ногу з часом. Проте накопичення інформації – це не єдине, на що потрібно звернути увагу. Існує також така проблема як захист інформації на підприємстві та управління інформаційною безпекою підприємства. Для цього необхідно оцінити ризики та можливі причини втрати цінної для підприємства інформації. Після того, як ризики будуть оцінені, необхідно виконати ряд дій по нормативам управління інформаційною безпекою підприємства. Для цього існують певні заходи. Якщо дотримуватись правил управління інформаційними ресурсами, то можна уникнути ситуацій втрати інформації. Фахівці з управління інформаційною безпекою здатні вирішувати завдання теоретичного та практичного характеру, що безпосередньо пов'язані з усіма аспектами захисту інформації. Отже грамотна інформаційна безпека – це складова, яка дозволить підприємству залишатися на високому рівні і бути конкурентоспроможним та успішним.

Література:

1. Інформаційна безпека // Економічний енциклопедичний словник. [Електронний ресурс]. – Режим доступу: http://zalik.org.ua/index.php?newsid=25011

2. Шевченко С.Ю. Формування системи управління інформаційної безпеки підприємства / С.Ю. Шевченко // Економіка підприємства: теорія та практика: зб. мат. IV міжнар. наук.- практ. конф. 12 жовт. 2012р., - К.: КНЕУ, 2012.

3. Чунарьова А.В. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO / А.В. Чунарьова, А.В. Чунарьов // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: науково-технічний збірник. – К.: НТУУ "КПІ" , 2012. – № 2(24). – С.50-53.