УДК 004.056.53

Грінченко Є. М., Колмик О. О.
Харківський національний університет внутрішніх справ

Методи управління інформаційними ризиками

У світлі розвитку інформаційних технологій потреба в захисті інформації зростає з кожним днем. Але обробка, передача та захист інформації пов'язані з ризиком, який необхідно враховувати, оцінювати і управляти для успішної роботи організації.

Не дивлячись на значну кількість різних класифікацій загроз у сфері інформаційної безпеки, в вивченій літературі відсутня встановлена класифікація інформаційних ризиків. Вони розглядаються як один з видів операційних ризиків підприємства.

Як правило, всі види інформаційних ризиків взаємопов'язані і впливають на діяльність підприємства. При цьому зміна одного виду ризику може викликати зміну більшості інших.

Класифікація ризиків означає об'єднання сукупності ризиків на підставі певних ознак і критеріїв. Такими критеріями, покладеними в основу класифікації інформаційних ризиків, є:

−основні аспекти інформаційної безпеки;

−час виникнення;

−джерело виникнення;

−природа інформаційного активу;

−характер загрози інформаційної безпеки;

−характер наслідків; механізм впливу.

Основними аспектами інформаційної безпеки є: доступність, цілісність і конфіденційність інформації.

Під доступністю розуміється можливість доступу суб'єкта до даних за запитом в будь-яке передбачене розкладом роботи час. Можливість отримання даних за запитом залежить від працездатності та завантаженості елементів інформаційної системи і її каналів передачі даних.

Ризик порушення доступності інформації може залежати як від несправності обладнання і збоїв в програмному забезпеченні в компанії, так і від успішно реалізованих мережевих атак на інформаційну систему із зовні.

Даний тип ризику безпосередньо залежить від надійності апаратних і програмних компонентів інформаційної системи, а так само від рівня компетенцій персоналу, керуючого їх роботою. Порушення доступності так само виникають через недотримання вимог різних стандартів як на етапі проектування так і на етапах виробництва або експлуатації системи.

Під цілісністю розуміється актуальність і несуперечність інформації, рівень її захисту від руйнування і несанкціонованого зміни і видалення.

Ризик порушення цілісності забезпечується можливостями відмови обладнання і програмного забезпечення, ступенем продуманості алгоритмів і надійністю засобів доступу користувачів системи, які мають право на редагування інформації, ймовірністю наявності в системі недокументованих можливостей, недосконалістю організаційної структури ІС, а так само недодержанням вимог стандартів на етапі проектування, виробництва і експлуатації системи.

Під конфіденційністю розуміється рівень захисту інформації від несанкціонованого доступу.

Ризик порушення конфіденційності так само залежить від рівня алгоритмів аутентифікації користувачів, ймовірністю наявності недокументованих ситуацій при

роботі з ІС, недосконалістю організаційної структури, недотриманням стандартів і людським фактором.

За часом виникнення інформаційні ризики розподіляються на ретроспективні, поточні та перспективні ризики. Аналіз ретроспективних ризиків, їх характеру і методів їх мінімізації дозволяє точніше прогнозувати поточні і перспективні ризики.

За середовищі виникнення ризики діляться на зовнішні і внутрішні.

На зовнішні ризики не впливає внутрішня складова підприємства, вони не пов'язані з прямою діяльністю підприємства і ніяк не може вплинути на їх рівень. Їх рівень обумовлений політичною обстановкою в країні і між державами, економічною ситуацією на ринку, соціальним рівнем громадян і т.д.

До внутрішніх інформаційних ризиків відносяться ризики, які залежать від безпосередньої діяльності підприємства і його персоналу. На їх рівень можуть впливати наступні фактори: виробничий потенціал організації, рівень технічного оснащення, ступінь кваліфікації персоналу, наявність засобів захисту інформації, наявність посадових інструкцій при роботі з ІС.

За природою інформаційного активу інформаційні ризики можна розділити на ризики апаратні і програмні. Апаратні ризики виникають при виході з ладу комплексів ІС, таких як: сервери, персональні комп'ютери, мережеві комутатори і маршрутизатори, виробниче обладнання, верстати і т.д. Програмні ризики безпосередньо пов'язані зі збоями в роботі програмного забезпечення підприємства, дії шкідливого програмного забезпечення, операційних систем користувачів ІС, а так само пов'язані з витоком інформації і дії мережевих атак. Формуючи класифікацію, пов'язану з характером загрози інформаційній безпеці, можна виділити наступні ризики:

Організаційні ризики - це ризики, пов'язані діяльністю персоналу, що експлуатує і обслуговує ІС, проблемами системи внутрішнього контролю, погано розробленими правилами робіт, тобто ризики, пов'язані з внутрішньою організацією роботи компанії.

Технічні ризики пов'язані з обладнанням, програмним забезпеченням, їх завданнями, способами проектування, розробки та експлуатації ІС. Ці ризики безпосередньо пов'язані з життєвим циклом ІС.

До природних інформаційним ризиків відносяться ризики, що не залежать від діяльності людини. Вони здатні завдати шкоди, який можемо привести до повної зупинки функціонування підприємства. Вони пов'язані з діяльністю природних явищ, таких як землетруси, повені, шторми, урагани, і т.д.

Найчастіше ризик характеризується сукупністю трьох якостей: наявністю джерела небезпеки; невизначеністю настання небезпечної події; можливістю заподіяння шкоди. Отже, управляти ризиком - це значить:

– виявляти, вивчати, усувати, нейтралізовувати або зменшувати джерела небезпеки;

– здійснювати систематичний моніторинг і прогнозувати сценарії розвитку небезпечних подій;

– запобігати, локалізувати і усувати негативні наслідки небезпечних подій.

Пропонуються основні методи управління інформаційними ризиками:

– зниження (удосконалення заходів щодо запобігання небезпечних ситуацій, розробка систем їх локалізації);

– прийняття (підготовка фінансових і матеріальних резервів на випадок реалізації небезпечних ситуацій);

– передача (страхування або інші механізми фінансування ризику);

– виключення (перехід на менш небезпечні технології, удосконалення захисних програм, і т. д.).