Розділ 2. Методика оцінювання ризику

Щоби оцінити ризик, зручно використовувати простий і зрозумілий метод розрахунку. Саме простота дає змогу достовірно оцінити ризики і за необхідності корегувати їх значення. Найпростішою є формула:

*Ризик=Ймовірність\*Збиток*

**2.1. Методика оцінки ймовірності реалізації загрози.**

Оцінка ймовірності реалізації загрози здійснюється за непрямим показниками, а саме:

* можливість виникнення джерела ,що визначає міру доступності до можливості використати фактор (уразливість) (для антропогенних джерел), віддаленість від фактора (уразливості) (для техногенних джерел) або особливості обстановки (для випадкових джерел);
* готовність джерела , що визначає міру кваліфікації та привабливість здійснення діяння з боку джерела загрози (для антропогенних джерел) або наявність необхідних умов (для техногенних та стихійних джерел);
* фатальність , що визначає міру непереборності наслідків реалізації загрози.

Кожний показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Коефіцієнт  для окремого джерела можна визначити як відношення добутку наведених вище показників до максимального значення 125:



*Табл. 2.1*

Розділ 3. Оцінювання ризиків.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Електронний каталог лотв (містить інформацію про технічні характеристики продукції, її  ціну, включаючи плату за доставку, та умови оплати) | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступності | Адміністратор веб-сервера | Дата центр  Компанії «Data group» | БД | Хакер | DDoS-напад на сервер, що містить інформацію через *відсутність фільтрації трафіку.* | 5 | 4 | 2 | 0,32 | 1 | 13 |
| Знищення інформації за рахунок XSS-нападу на ПЗ веб-сайту через *відсутність екранування вхідних даних* | 2 | 4 | 4 | 0,25 | 4 | 39 |
| Системний адміністратор | Знищення інформації за рахунок використання робочого місця адміністратора веб-сервера через *відсутність виходу з системи, коли залишається робоче місце* | 4 | 4 | 4 | 0,51 | 4 | 80 |
| Цілісності | Системний адміністратор | Модифікація інформації про ціну товару за рахунок використання робочого місця адміністратора веб-сервера через *відсутність виходу з системи, коли залишається робоче місце* | 4 | 3 | 2 | 0,19 | 2 | 15 |
| Хакер | Модифікація інформації про ціну товару за рахунок XSS-нападу на ПЗ веб-сайту через *відсутність екранування вхідних даних* | 5 | 4 | 4 | 0,64 | 4 | 100 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Програмне забезпечення інтернет магазину | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Адміністратор веб-сервера | Дата центр Компанії «Data group» | ПЗ | Хакер | DDoS-напад на сервер, що містить ПЗ через відсутність фільтрації трафіку. | 5 | 4 | 2 | 0,32 | 1 | 13 |
| Системний адміністратор | Видалення ПЗ за рахунок використання робочого місця адміністратора веб-сервера через відсутність виходу з системи, коли залишається робоче місце | 4 | 4 | 4 | 0,51 | 4 | 80 |
| Цілісність | Хакер | Модифікація ПЗ за рахунок XSS-нападу на ПЗ веб-сайту через відсутність екранування вхідних даних | 5 | 4 | 4 | 0,64 | 4 | 100 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Електронні відомості про проведення аукціону (П.І.Б., контактний телефон,e-mail, адреса проживання, перелік замовлених товарів ) | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Консультант | Сервер 1 | БД | Основний персонал компанії | Знищення інформації за рахунок привласнення ідентифікатора системного адміністратора, який необхідний для роботи з системою 1С через *ненадійність ідентифікатора системного адміністратора (мала довжина, використання стандартних комбінацій)* | 3 | 3 | 2 | 0,14 | 3 | 16 |
| Блокування доступу інших користувачів до інформації за рахунок видалення або зміни їх облікових записів для доступу до системи 1с шляхом привласнення ідентифікатора системного адміністратора, який необхідний для роботи з обліковими записами користувачів в системі 1С через  *ненадійність ідентифікатора системного адміністратора (мала довжина, використання стандартних комбінацій)* | 3 | 2 | 2 | 0,09 | 1 | 4 |
| аміністартор веб-сервера | Знищення інформації за рахунок використання робочого місця системного адміністратора через *відсутність виходу з системи, коли залишається робоче місце* | 4 | 3 | 2 | 0,19 | 3 | 22 |
| Блокування доступу інших користувачів до інформації за рахунок видалення або зміни їх облікових записів для доступу до ситеми 1С шляхом використання робочого місця системного адміністратора через *відсутність виходу з системи, коли залишається робоче місце.* | 4 | 3 | 2 | 0,19 | 1 | 7 |
| Хакер | Знищення інформації за рахунок проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей) | 2 | 4 | 2 | 0,12 | 3 | 14 |
| Блокування доступу інших користувачів до інформації за рахунок видалення або зміни їх облікових записів для доступу до ситеми 1С шляхом проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей) | 2 | 3 | 2 | 0,09 | 1 | 4 |
| Лінія електроживлення | Знищення інформації за рахунок виходу з ладу сервера внаслідок перепаду напруги через *відсутність стабілізатора напруги* | 4 | 3 | 4 | 0,38 | 4 | 59 |
| Блокування доступу до інформації, за рахунок відсутності електроживлення сервера через *відсутність джерела безперебійного живлення* | 4 | 2 | 2 | 0,13 | 1 | 5 |
| Пожежа | Знищення інформації через фізичне знищення сервера внаслідок пожежі, яка виникла через  *відсутність пожежної сигналізації.* | 3 | 2 | 4 | 0,19 | 4 | 30 |
| Цілісніть | Основний персонал компанії | Модифікація інформації за рахунок привласнення ідентифікатора менеджера з продажу, який необхідний для роботи з системою 1С через *ненадійність ідентифікатора (мала довжина, використання стандартних комбінацій)* | 3 | 4 | 3 | 0,29 | 2 | 23 |
| Хакер | Віддалена модифікація інформації за рахунок проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей) | 2 | 4 | 3 | 0,19 | 2 | 15 |
| Конфіденційність | Основний персонал компанії | Копіювання інформації на сторонні носії через *відсутність обмеження на використання стороніх носіїв інформації* | 4 | 3 | 1 | 0,09 | 5 | 18 |
| Працівники компанії «Київстар» | Перехоплення інформації яка надходить з веб-сайту через мережу інтернет за рахунок *незахищеного з’єднання.* | 2 | 2 | 1 | 0,03 | 5 | 6 |
| Хакер | Викрадення інформації за рахунок проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей)*.* | 2 | 4 | 1 | 0,06 | 5 | 12 |

x

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Інформація в електронному вигляді про наявні на складі товари (Назва, категорія, модель, марка, технічні характеристики) | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Оператор поштового відділу | Сервер 1 | БД | Хакер | Зараження корпоративного сервера вірусом-шифрувальником через *відсутність брандмауера для захисту локальної мережі від шкідливого трафіку.* | 3 | 3 | 2 | 0,14 | 2 | 11 |
| Цілісність | Персонал підприємства | Внесення змін в інформацію про товари, які суперечать посадовим інструкціям через *відсутність політики розмежування доступу.* | 4 | 2 | 2 | 0,13 | 2 | 10 |
| Хакер | Модифікація інформації про товари через *відсутність брандмауера для захисту локальної мережі від шкідливого трафіку.* | 3 | 3 | 2 | 0,14 | 2 | 11 |
| Конфіденційність | Хакер | Копіювання інформації з сервера через  *відсутність брандмауера для захисту локальної мережі від шкідливого трафіку.* | 3 | 4 | 3 | 0,29 | 1 | 11 |
| Персонал підприємства | Копіювання інформації на сторонні носії зберігання данних через  *відсутність обмеження на використання стороніх носіїв інформації.* | 4 | 3 | 3 | 0,29 | 1 | 11 |
| Системний адміністатор | Надання доступу до інформації стороннім особам через зміну *конфігурації мережного обладнання.* | 5 | 4 | 3 | 0,48 | 1 | 19 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сервер 1 | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Системний адміністратор | Серверна | КТ | Хакер | Зараження корпоративного сервера вірусним ПЗ через *відсутність антивірусного захисту,* яке спричиняє збої в роботі сервера. | 3 | 4 | 3 | 0,29 | 2 | 23 |
| Система кондціонування | Знищення інформації через перегрівання сервера за рахунок *виходу з ладу системи кондиціонування* | 3 | 3 | 4 | 0,29 | 4 | 45 |
| Лінія електроживлення | Знищення інформації за рахунок виходу з ладу сервера внаслідок перепаду напруги через *відсутність стабілізатора напруги* | 4 | 3 | 4 | 0,38 | 4 | 59 |
| Блокування доступу до інформації, за рахунок відсутності електроживлення сервера через *відсутність джерела безперебійного живлення* | 4 | 2 | 2 | 0,13 | 1 | 5 |
| Пожежа | Знищення інформації через фізичне знищення сервера внаслідок пожежі, яка виникла через  *недотримання правил пожежної безпеки та відсутність пожежної сигналізації.* | 3 | 2 | 4 | 0,19 | 4 | 30 |