Министерство науки и высшего образования Российской Федерации

**Федеральное государственное бюджетное образовательное учреждение**

**высшего профессионального образования**

«Владимирский государственный университет

имени Александра Григорьевича и Николая Григорьевича Столетовых»

**(ВлГУ)**

**Кафедра информационных систем и программной инженерии**

Практическая работа №3

по дисциплине «Основы информационного менеджмента»

Тема работы:

Анализ и оценка информационных рисков

Выполнил:

студент гр. ПРИ-120

Парахин К.В.

Принял:

Хорошева Е.Р.

Владимир 2024 г.

Цель работы:

Выполнить анализ информационных рисков, обосновать использование количественного/качественного метода для оценки разных видов риска и выполнить оценку рисков на примере предприятия.

Ход работы:

На примере компании ООО «АИСТСОФТ»:

1. идентифицировать риски
2. обосновать использование количественного/ качественного метода для оценки разных видов риска
3. оценить информационные риски:

* Количественным методом
* Качественным методом

ВЫПОЛНЕНИЕ РАБОТЫ

Организация: ООО «АИСТСОФТ» города Владимир.

Тема ВКР: Разработка корпоративной системы для организации работы IT-отделов предприятия (ПИС «Органайзер предприятия»).

«Органайзер предприятия» - это кросс-платформенное (мобильное и WEB – приложение), предоставляющее возможности по организации корректной и стабильной работы IT-отделов предприятия.

Возможны следующие риски:

1. несанкционированный доступ к информационным ресурсам;
2. незаконное копирование данных в информационных системах;
3. доступ к функционалу системы уволенными сотрудниками
4. сбой аппаратного обеспечения;
5. сбой программного обеспечения;
6. манипулирование информацией (дезинформация, сокрытие или искажение информации);
7. утечка персональных данных;
8. порча хранимых данных.

Воспользуемся количественным методом оценки для следующих рисков:

1. сбой аппаратного обеспечения;
2. сбой программного обсечения;
3. утечка персональных данных;
4. порча хранимых данных;

т.к. этот метод дает наглядное представление в денежном выражении по объектам оценки (ущербу, затратам).

Воспользуемся качественным методом для оценки таких рисков, как:

1. несанкционированный доступ к информационным ресурсам;
2. незаконное копирование данных в информационных системах;
3. доступ к функционалу системы уволенными сотрудниками
4. манипулирование информацией (дезинформация, сокрытие или искажение информации);

т.к. для данных видов рисков нельзя получить представление в денежном выражении о размере ущерба, затрат и выгод от внедрения СЗИ.

1. Применение количественного метода оценки

Для оценки рисков количественным методом необходимо выяснить потенциальный ущерб каждой угрозы и частоту возникновения угрозы. Данные представлены в таблице 1.

Таблица 1 – Оценка рисков количественным методом

|  |  |  |  |
| --- | --- | --- | --- |
| Риск | Разовый ущерб, руб. | Частота возникновения, в год | Среднегодовой ущерб |
| сбой аппаратного обеспечения | 100 000 1 | 3 | 300 000 |
| сбой программного обеспечения | 35 000 2 | 12 | 90 000 |
| утечка персональных данных | 50 000 3 | 1 | 50 000 |
| порча хранимых данных | 200 000 4 | 1 | 200 000 |
|  |  |  | 540 000 |

1 стоимость разового ущерба от прямого выхода сервера из строя

2 стоимость разового ущерба от простоя системы, вызванного сбоем в программном обеспечении

1. КоАП РФ Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных, часть 6: «Невыполнение требований по сохранности и ограничению доступа к данным»

4 УК РФ Статья 146. Нарушение авторских и смежных прав: «Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю» или «Незаконное использование объектов авторского права или смежных прав».

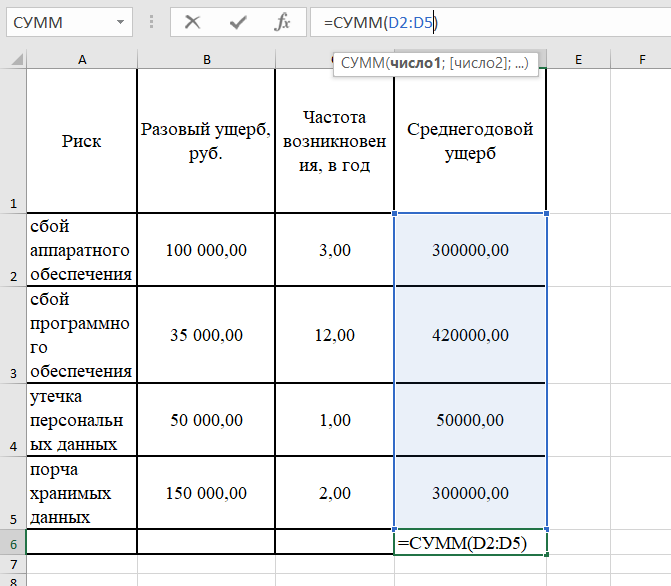


Рисунок 1. Выполнение расчетов для количественных методов оценки

Анализ полученных данных по ущербу для каждой угрозы и способы их минимизации:

1. Чтобы минимизировать риски сбоя аппаратного обеспечения, необходимо внедрение системы бесперебойного питания и системы резервного копирования информации, а также необходимо закупать оборудование только у надежных производителей.

Общая стоимость обновления составит 150 000 рублей – что в рамках годового обслуживания старой системы будет выгоднее, чем терпеть расходы по 300000 руб. ежегодно;

1. Чтобы минимизировать риски сбоя программного обеспечения, необходимо следить за обновлениями ПО, использовать только лицензионное ПО;
2. Чтобы минимизировать риск утечки персональных данных и порчи хранимых важных данных, необходимо использование средств криптографической защиты для шифрования данных при хранении и передаче, использование цифровых подписей (50 000 рублей на 1 сервер), использование средств антивирусной защиты (10 000 рублей в год), а также необходимо создавать и использовать дополнительные backup-сервера с дублирующимися базами данных (500000 руб. за каждый сервер, всего серверов – 5 – что будет выгоднее и надежнее, чем терпеть ежегодные потери прибыли из-за порчи хранимых данных в размере в среднем около 300000 рублей в год).
3. Применение качественного метода оценки

Для оценки рисков качественным методом необходимо выявить ценность информационных активов и выявить вероятность и последствия возможных угроз.

Ценность информационных активов будем определять по уровню критичности (последствиям) при нарушении характеристик безопасности (1 – незначительная, 2 – существенная, 3 – критичная).

Для оценки вероятности реализации угрозы используется трехуровневая качественная шкала (низкая, средняя, высокая).

Для оценки уровня возможности реализации угрозы также может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

Для определения уровня риска можно использовать пятибалльную шкалу (1 – минимальный уровень риска, 5 – высокий уровень риска).

Данные представлены в таблице 2.

Таблица 2 – Оценка рисков качественным методом.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Риск | Ценность информационных активов | Вероятность реализации угрозы | Возможность успешной реализации угрозы | Уровень информационного риска |
| несанкционированный доступ к информационным ресурсам | существенная | средняя | средняя | 3 |
| незаконное копирование данных в информационных системах | критичная | средняя | средняя | 4 |
| доступ к функционалу и данным системы уволенными сотрудниками | критичная | высокая | средняя | 4 |
| манипулирование информацией (дезинформация, сокрытие или искажение информации) | критичная | низкая | низкая | 3 |

Анализ полученных данных по ущербу для каждой угрозы и способы их минимизации:

1. Риск несанкционированного доступа может привести к потере важной информации. Для минимизации риска - необходимо внедрить средства физической защиты, а также постоянно обновляемую и проверяемую систему политик безопасности, систему резервного копирования, предоставляющую возможность совершать backupы уже имеющихся данных – на случаи возникновения неприятностей.
2. Риск незаконного копирования данных может привести к распространению как конфиденциальной информации, так и других видов информации. Для минимизации рисков необходимо ввести систему цифровых подписей, использовать шифрование. Также есть опция для ввода дополнительных систем криптографии – что рассматривалось в одном из рисков из прошлой группыю
3. Риск доступа к функционалу и данным системы со стороны уволенных сотрудников может приводить к утечке важной коммерческой информации компании, доступа к интеллектуальной собственности компании и ее сотрудников. Риск возникновения такой угрозы достаточно велик, так как ежегодно могут быть уволены по некоторой причине до 12 сотрудников из компании. Для минимизации риска – необходимо проводить полный алгоритм очистки рабочего ПК сотрудника, деактивации его учетной записи и аккаунтов в рабочих приложениях – и провести генерацию новых криптографических данных (в случае его повторного трудоустройства в компанию).
4. Риск манипулирования информацией также может нанести значительный ущерб. Мерами по предотвращению таких рисков может стать резервное копирование, фиксирование произведенных изменений.

ВЫВОД

В процессе выполнения работы мною был выполнен анализ информационных рисков, обосновано использование количественного/качественного метода для оценки разных видов риска и выполнена оценка рисков на примере IT - предприятия ООО «АИСТСОФТ» г. Владимира.