Министерство образования и науки 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 «АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ»

Выполнила:

студент гр. ИСТ-120

Вылегжанина Е.Н.

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.

ЗАДАНИЕ

На примере компании: Altenar.

1) идентифицировать риски

2) обосновать использование количественного/ качественного метода для оценки разных видов риска

3) оценить информационные риски:

• Количественным методом

• Качественным методом

ВЫПОЛНЕНИЕ РАБОТЫ

Предметная область: Altenar.

Возможны следующие риски:

1) несанкционированный доступ к информационным ресурсам;

2) незаконное копирование данных в информационных системах;

3) сбой аппаратного обеспечения;

4) сбой программного обсечения;

5) манипулирование информацией (дезинформация, сокрытие или искажение информации);

6) утечка персональных данных;

7) хищение интеллектуальной собственности.

Воспользуемся количественным методом оценки для следующих рисков:

1) сбой аппаратного обеспечения;

2) сбой программного обсечения;

3) утечка персональных данных;

4) хищение интеллектуальной собственности.

Воспользуемся качественным методом для оценки таких рисков, как:

1) несанкционированный доступ к информационным ресурсам;

2) незаконное копирование данных в информационных системах;

3) 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 | Среднегодовой ущерб |
| сбой аппаратного обеспечения | 150 000 1 | 3 | 450 000 |
| сбой программного обеспечения | 50 000 2 | 4 | 200 000 |
| утечка персональных данных | 100 000 3 | 1 | 100 000 |
| хищение интеллектуальной собственности | 100 000 4 | 1 | 100 000 |
|  |  |  | 850 000 |

1 стоимость разового ущерба от прямого выхода системы из строя

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

3 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».

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.

2) Чтобы минимизировать риски сбоя программного обеспечения, необходимо следить за обновлениями ПО, использовать только лицензионное ПО;

3) Чтобы минимизировать риск утечки персональных данных и хищения интеллектуальной собственности, необходимо использование средств криптографической защиты для шифрования данных при хранении и передаче, использование цифровых подписей (40 000 рублей на 1 сервер), использование средств антивирусной защиты (60 000 рублей в год).

2. 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 | критичная | низкая | средняя | 3 |
| Незаконное копирование данных в информационных системах | критичная | средняя | низкая | 4 |
| Манипулирование информацией (дезинформация, сокрытие или искажение информации) | критичная | низкая | средняя | 5 |

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.

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.

3) Риск манипулирования информацией также может нанести значительный ущерб. Мерами по предотвращению таких рисков может стать шифрование данных и выдача данных по паролю.

ВЫВОДЫ

В процессе выполнения работы был выполнен анализ информационных рисков, обосновано использование количественного/качественного метода для оценки разных видов риска и выполнена оценка рисков на примере предприятия.