МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ государственное БЮДЖЕТНОЕ

образовательное учреждение

высшего образования

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет автоматики и вычислительной техники

Кафедра защиты информации

**

**ОТЧЁТ**

**по расчётно-графическому заданию**

**«Оценка рисков информационной безопасности предприятия малого бизнеса»**

по дисциплине: «Основы информационной безопасности»

Выполнил: ФИОПреподаватель:

студент гр. АВТ-918 Харюткина С.А.

«\_\_\_» \_\_\_\_\_\_\_\_\_ 2022 г.«\_\_\_» \_\_\_\_\_\_\_\_\_ 2022г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(оценка, подпись)

Новосибирск

2022

**Цель работы**

Основной целью данной работы является получение оценки состояния защищённости информации в выбранном нами предприятии, оценки возникновения различного рода угроз, расчёт, возможных потерь от этих угроз, расчёт потерь на используемые средства безопасности и оценка эффективности этих средств в финансовом плане.

**Введение**

В качестве исследуемой компании, выберем предприятие из сферы малого бизнеса ООО "ЭрСи Медикал". Краткое описание компании:

Данная компания 9 лет специализируется на коммерческих медицинских услугах.

Организация находится по адресу г. Новосибирск ул. Советская, 50 и   
ул. Гоголя, 38

**Методика оценки угроз и их устранения**

Рассматриваемая методика предназначена для проведения анализа возможных возникающих угроз информационной безопасности сети данной компании и сведения их к минимуму наиболее экономными средствами.

В основе выбранной методики лежит оценка и учёт наиболее вероятных угроз для данной информационной сети данной компании, исходя из сведений о ней, оценка наносимого ущерба от каждого вида угрозы, а также оценка суммарных потерь от возникающих угроз. Следующим этапом является оценка финансовых потерь на средства преодоления этих угроз: тех, которые уже использует компания, и дополнительных рекомендованных средств. И в завершении приведём обусловленность применения данных средств для защиты информационной сети компании, а именно оценим получаемую выгоду от использования данных средств для защиты информационной сети компании.

Алгоритм данной методики:

1. Идентификация активов компании.
2. Разработка модели угроз.
3. Идентификация возникающих угроз по степени вероятности их возникновения.
4. Оценка имеющихся средств защиты у данной компании.
5. Оценка наносимого ущерба каждой из этих угроз с учётом частоты её возникновения, а также используемых средств защиты информации направленных конкретно против этой угрозы.
6. Оценка получаемой выгоды от этих средств защиты.
7. Приведение дополнительных рекомендованных средств защиты.
8. Оценка получаемой выгоды от дополнительных средств защиты.
9. Выводы.

Следуя этому алгоритму, проведём исследования для выбранной нами компании.

**Идентификация активов компании**

Среди активов компании ООО "ЭрСи Медикал" можно выделить следующие:

* Штат сотрудников, насчитывающий 63 человек
* Компьютеры
* Сервер
* Различного рода программы, в частности, для исследования различных показателей здоровья
* Телефоны
* Базы данных
* Продукция компании
* Носители информации
* Документация

**Модель возникающих угроз, степени их угроз, частота возникновения и меры противодействия им**



**Имеющиеся средства защиты.**

У компании "ЭрСи Медикал" используется бесплатное антивирусное ПО AVAST. В информационной системе предприятия используются пароли, в среднем состоящие из 12 символов, использующих 70 знаков. VPN в компании не используются, системы сигнализации и камеры видеонаблюдения установлены в количестве 12 штук, стоимость обслуживания которых составляет 43 200 в год. Политика безопасности в компании не была разработана, инструктажи работников проводятся редко. Таким образом, можно сказать, что у данной компании информационная сеть является не защищённой.

**Оценка наносимого ущерба от каждого вида угроз при имеющейся защите**

Оценку наносимого ущерба от вышеперечисленных угроз сделаем, исходя из частоты появления этой угрозы и наносимого ей ущерба в финансовом плане. Воспользуемся эмпирической зависимостью, выражающую общие потери от данной угрозы i:

, где Si–коэффициент частоты появления угрозы, Vi–коэффициент наносимого ущерба от данной угрозы, Ri–ущерб, нанесённый данной угрозой.

Значения коэффициентов Siи Viвозьмём из следующих таблиц:

|  |  |
| --- | --- |
| **Возможная частота появления угрозы** | **Предполагаемое значение Si** |
| Почти никогда | 0 |
| Раз в 1000 лет | 1 |
| Раз в 100 лет | 2 |
| Раз в 10 лет | 3 |
| Раз в год | 4 |
| Раз в месяц | 5 |
| 1-2 раза в неделю | 6 |
| 3 раза в неделю | 7 |

|  |  |
| --- | --- |
| **Возможный ущерб при возникновении угрозы (руб.)** | **Предполагаемое значение Vi** |
| 1 | 0 |
| 10 | 1 |
| 100 | 2 |
| 1 000 | 3 |
| 10 000 | 4 |
| 100 000 | 5 |
| 1 000 000 | 6 |
| 10 000 000 | 7 |

Найдём ущерб, нанесённый каждой из вышеперечисленных угроз, исходя также из того, что информационная сеть данной компании является частично защищённой:

1. Компьютерные вирусы. Поскольку данная компания имеет средства антивирусного ПО AVAST, то её информационной сеть заражается вирусами в среднем раз в 1-2 раза в месяц, ущерб нанесённым таким заражением оценивается в 10 000 рублей. Ущерб, нанесённый данной угрозой, составит:

R1 = 10(6 + 3 - 4) = 105 = 100 000 рублей

1. Взлом паролей. Сотрудники компания используют пароли, состоящие в среднем из 12 символов, использующих 70 знаков. Вероятность подбора пароля составляет 1 раз в месяц, наносимый ущерб от взлома пароля составляет 1000 рублей. Ущерб, наносимый данной угрозой, составляет:

R2 = 10(5 + 3 - 4) = 104 = 10 000 рублей

1. Взлом криптозащиты. Компания не использует криптограф. Взлом криптозащиты в среднем происходит раз в 10 лет, наносимый ущерб составляет 10 000 рублей. Ущерб, наносимый данной угрозой, составляет:

R3 = 10(4 + 3 – 4) = 103 = 1000 рублей.

1. DOS/DDOSатаки. Не используется защита. Эти атаки происходят в среднем раз в год, наносимый ущерб составляет 10000 рублей. Ущерб, наносимый данной угрозой, составляет:

R4 = 10(4 + 4 - 4) = 104 = 10 000 рублей

1. Троянские программы. Вероятность заражения троянской программой составляет в среднем 1-2 раза в месяц, наносимый ущерб от одного заражения оценивается в 1000 рублей. Ущерб, наносимый данной угрозой, составляет:

R5 = 10(5 + 3 - 4) = 104 =10 000 рублей

1. Логические бомбы. Частота поражения системы данной угрозой составляет примерно 1 раз в 100 лет, наносимый ущерб от одной атаки оценивается в 1000 рублей. Ущерб, наносимый данной угрозой:

R6 = 10(4 + 2 - 4) = 102 = 100 рублей

1. Перехват информации. Поскольку компания не использует средств для защиты от данной угрозы, например, те же VPN, то частота появления угрозы составляет 1 раза в год, наносимый ущерб составляет 100 рублей. Ущерб, наносимый данной угрозой:

R7 = 10(2+ 4 – 4) = 102 = 100 рублей

1. Срыв связи. В среднем срыв связи происходит 1 раз в месяц, наносимый ущерб от одного срыва составляет 10 рублей. Ущерб, наносимый угрозой:

R8 = 10(5 + 1 - 4) = 102 = 100 рублей

1. Перехват ПЭМИН. Перехват ПЭМИН происходит достаточно редко – примерно раз в 10 лет, наносимый ущерб составляет примерно 1000 рублей от одного перехвата. Ущерб, наносимый угрозой:

R9 = 10(3 + 3 – 4) = 102 = 100 рублей

1. Хищение носителей информации и документации. Данные вид угроз чаще возникает от людей, не принадлежащих данной компании. Из средств защиты установлены видеокамеры и сигнализация. Однако учитывая, расположения офиса не в своём отдельном здании, а в бизнес-центре, данная угроза вполне имеет место быть от других людей, работающих в этом центре или посещающих его. Можно сказать, что в среднем хищение носителей информации происходит раз в месяц. Ущерб от похищения документа или носителя информации сильно различается, в зависимости от степени важности информации и её конфиденциальности. Скажем так, что в среднем хищение носителей информации или документов обходится компании в 1000 рублей. Таким образом, получаем что ущерб, нанесённый данной угрозой, оценивается следующей суммой:

R10 = 10(4 + 3 - 4) = 103 = 1 000 рублей

Подсчитаем общие убытки компании из-за возникающих угроз по формуле:

Суммарные убытки компании из-за угроз информационной сети:

R = 100 000 + 10 000 + 1000 + 10 000 + 10 000 + 100 + 100 + 100 + 100 + 1 000 = 130 400 рублей

**Оценка наносимого ущерба от каждого вида угроз при отсутствии защиты**

Приведём убытки компании от каждой угрозы, если бы она вообще не имела средств защиты. Убытки были бы те же самые, возрастём только частота возникновения угроз:

1. Компьютерные вирусы. Заражение в этом случае происходило бы в среднем 1-3 раза в неделю.

R1 = 10(7 + 3 - 4) = 106 = 1000 000 рублей

1. Взломы паролей. Подбор паролей происходит в среднем 1 раз в месяц.

R2 = 10(5 + 3 - 4) = 104 = 10 000 рублей

1. Взлом криптозащиты. Затраты также останутся примерно теми же.

R3 = 10(4 + 3 – 4) = 103 = 1000 рублей.

1. DOS/DDOSатаки. Затраты также останутся примерно теми же.

R4 = 10(4 + 4 - 4) = 104 = 10 000 рублей

1. Троянские программы. Вероятность заражение троянскими программами составляет 1-2 раза в неделю.

R5 = 10(6 + 3 - 4) = 105 =100 000 рублей

Потери от остальных угроз будут примерно теми же.

Суммарные возможные убытки компании при отсутствии средств защиты информационной сети:

R = 100 000 + 10 000 + 1000 + 10 000 + 100 000 + 100 + 100 + 100 + 100 + 1 000 = 230 400 рублей

**Рекомендованные дополнительные средства защиты**

В качестве дополнительных мер защиты можно использовать виртуальные частные сети VPN, стоимость обслуживания одного компьютера составляет 550 рублей, таким образом, для 25 компьютеров стоимость будет составлять 13 750 рублей в год. Можно использовать более надёжные пароли, состоящие более чем из 12 символов, при использовании 70 знаков. Серьёзной проблемой в безопасности данной информационной сети является слабое антивирусное ПО по сравнению с платным, поэтому будет установлено антивирусное ПО Kaspersky Small Office Security для каждого компьютера, общая стоимость будет составлять 28 950. И, наконец, в качестве дополнительных мер защиты необходимо составить политику безопасности предприятия и проводить инструктажи работникам компании.

**Оценка наносимого ущерба от каждого вида угроз при дополнительной защите**

Ущерб от угроз не изменится, но уменьшится их частота возникновения, из-за чего итоговые затраты уменьшатся.

1. Компьютерные вирусы. В такой системы заражение вирусами происходит в среднем раз в год.

R1 = 10(4 + 3 - 4) = 103 = 1000 рублей

1. Взлом паролей. Подбор паролей происходят в среднем раз в год т.к. в ПО Kaspersky Small Office Security присутствует менеджер паролей, безопасные платежи и резервное копирование данных

R2 = 10(4 + 3 - 4) = 103 = 1 000 рублей

1. Взлом криптозащиты. Затраты останутся примерно теми же.

R3 = 10(4 + 3 – 4) = 103 = 1000 рублей.

1. DOS/DDOSатаки. Эти атаки происходят в среднем раз в 10 лет, наносимый ущерб составляет 10000 рублей. Ущерб, наносимый данной угрозой, составляет:

R2 = 10(3 + 4 - 4) = 103 = 1 000 рублей

1. Троянские программы. Заражение троянскими программами происходит в среднем раз в год.

R5 = 10(4 + 3 - 4) = 103 = 1000 рублей

1. Логические бомбы. Потери от них примерно те же самые.

R6 = 10(4 + 2 - 4) = 102 = 100 рублей

1. Перехват информации. С использованием VPN число перехватов сокращается до 1 раза в год.

R7 = 10(1 + 4 - 4) = 101 = 10 рублей

1. Потери от срыва связи и перехвата ПЭМИН останутся примерно теми же:

R8 = 10(5 + 1 - 4) = 102 = 100 рублей

1. Перехват ПЭМИН. Перехват ПЭМИН происходит достаточно редко – примерно раз в 10 лет

R9 = 10(3 + 3 – 4) = 102 = 100 рублей

1. Хищение носителей информации и документации.

R10 = 10(3 + 3 - 4) = 103 = 1000 рублей

Суммарные возможные убытки компании при использовании дополнительных средств защиты информационной сети:

R = 1000 + 1000 + 1000 + 1000 + 1000 + 100 + 10 + 100 + 100 + 1000 = 6 310 рублей

**Оценка получаемой выгоды от используемых средств защиты**

Найдём численно получаемую выгоду при использовании имеющихся средств защиты в данной информационной системе и дополнительных средств. Для ещё рассчитаем затраты на средства защиты:

При использовании имеющихся средств защиты: S1 = 43 200 рублей в год

При использовании дополнительных средств защиты: S2 = 85 900 рублей в год.

Общие потери при отсутствии какой-либо защиты:

P1 =R = 230 400 рублей

Общие потери при частично защите информационной системы:

P2 = R + S1 =130 400 + 43 200 = 173 600 рублей

Общие потери при использовании средств дополнительной защиты:

P3 = R + S2 = 6 310 + 86 900 = 93 210рублей

**Выводы**

Исходя из полученных результатов можно сделать вывод, что даже при использовании имеющихся средств защиты общие потери значительно сокращаются - примерно в 1.3 раз. Потери сокращаются также при использовании средств дополнительной защиты, в 2.5. Из этого можно сделать вывод, что использование средств защиты информационной сети в современной компании крайне выгодно и необходимо для стабильной работы компании.