Учреждение образования

«Белорусский государственный технологический университет»

**Защита информации и надежность информационных систем**

**Лабораторная работа №1**

Разработка и внедрение политики безопасности организации или учреждения

Тип организации юридическая компания

Выполнил:

Студент 3 курса 2 группы ФИТ

Максимова Вера Владимировна

Проверил:

Ржеутская Надежда Викентьевна

**2022 г.**

1. **Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении).**

*Политика информационной безопасности* (ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

Актуальность ПИБ состоит в том, чтобы не допустить законодательно или на основе правил утечки конфиденциальной информации в свободный доступ. Для каждой организации или учреждения необходимо иметь собственный набор правил, составленных на основе законодательства РБ чтобы уменьшить риски и наложить ответственность в ответ на противоправные действия со стороны сотрудников или сторонних субъектов.

**Цели:**

* Разработка и внедрение политики безопасности для Юридической компании

**Задачи:**

* Установка объектов защиты
* Установка основных угроз и их источников
* Оценка угроз, рисков и уязвимостей
* Установка мер, методов и средств обеспечения требуемого уровня защищенности информационных ресурсов

1. **Объекты защиты.**

Юридическая компания.



Структура юридической компании:

* Директор
* Директор кадрового отдела
* Работник кадрового отдела
* Директор бухгалтерии
* Бухгалтер
* Юрист
* Специалист по работе с клиентами

1. **Основные угрозы и их источники.**

Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.

Внешние угрозы, влияющие:

* Атаки со стороны информационной безопасности
* Атаки со стороны конкурентов

Внутренние угрозы:

* Атаки со стороны сотрудников
* Разглашение информации о клиентах компетентными людьми

Непреднамеренные угрозы:

* Разговоры на тему работы
* Утеря носителей информации

Преднамеренные угрозы:

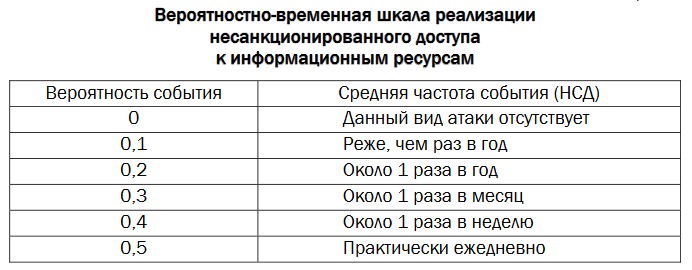
* Дезинформация
* Подделка документов
* Кража
* Угрозы сотрудникам, начальству, уборщикам помещений, арендодателям, заказчикам
* Восстановление удаленной информации с жестких дисков
* Несанкционированное распространение информации через поля и электрические сигналы

Естественные угрозы:

* Отсутствуют

1. **Основные угрозы и их источники.**

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации, не являющейся конфиденциальной и не раскрывающая данных о заказчиках |
| 1 | Ущерб атаки есть, но он незначителен и не связан с положением компании на рынке |
| 2 | Существует вероятность потери некоторого числа клиентов, компания теряет часть прибыли |
| 3 | Потеря весомой доли клиентов и потеря доли рынка, компания несет убытки |
| 4 | Полная потеря рынка и конкурентоспособности, долги, а так же полная потеря клиентов, банкротство |
| 5 | Полное банкротство компании и прекращение существования |



Условная численная шкала для оценки ущерба 0-5.

Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам 0-0,5.

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Подделка документов | 4 | 0.1 | 0.4 |
| Разговоры на тему работы | 2 | 0.3 | 0.6 |
| Атаки со стороны конкурентов | 3 | 0.1 | 0.3 |
| Атаки со стороны информационной безопасности | 3 | 0.2 | 0.6 |
| Разглашение информации о клиентах компетентными людьми | 3 | 0.1 | 0.3 |
| Атаки со стороны сотрудников | 3 | 0.1 | 0.3 |
| Итого | 6 | 0,15 | Сумма 2,5 |

Оптимальное значение коэффициента риска -- 0,3.

Критические значением считается 0,7, в случае его превышения финансовое состояние предприятия близко к банкротству.

Среднее значение риска вышло 0.42 – оптимальное.

1. **Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.**

* Установление норм и правил в договорах сотрудников о коммерческой тайне.
* Использование шифрования и защищенных сетей
* Использование специализированных ПО по утилизации цифровой информации или физическая утилизация жестких дисков при их замене в качестве издержек
* Исключение дезинформации и ее получение у соответствующих лиц
* Найм компетентных сотрудников

**Вывод:** юридическая компания “Бизнес-инфо” обладает относительно низким риском потери информации в любом из его проявлений, однако политика безопасности представленная выше при соблюдении оной всеми сотрудниками компании поможет снизить риск потери информации, либо же денежных средств до минимума.