МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования

«БЕЛОРУССКИЙ

ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий

Кафедра Информатики и веб-дизайна

Направление специальности Дизайн электронных и веб-изданий\_\_\_\_\_\_\_\_\_\_\_

**ОТЧЁТ**

**По лабораторной работе №1:**

**ТЕМА «РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ИЛИ УЧРЕЖДЕНИЯ»**

Минск 2021

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 Event-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.**

****

Структура расположения event-компаний – это офисы. Небольшие помещение способствуют меньшему риску со стороны количества персонала, но в то же самое время — это центральное место расположения компании. В основном компании арендуют офисы в специальных местах, где раздают помещения под офисные или рабочие пространства, соответственно существует угроза со стороны конкурентов и воровства коммерческой тайны.

Угроза выведения из строя компьютеров конкурентами или получение доступа к базам данных. Доступ к офису имеют: начальство, сотрудники, арендодатели и уборщики помещений (опционально).

Объекты защиты: ценные бумаги, компьютеры, сетевые каналы передачи информации.

Субъекты защиты: сотрудники и их контакты, заказчики.

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

Непреднамеренные угрозы:

* Отключение света
* Разговоры на тему работы

Преднамеренные угрозы:

* Атаки на сервер
* Перехват данных
* Кража
* Угрозы сотрудникам, начальству, уборщикам помещений, арендодателям, заказчикам
* Восстановление удаленной информации с жестких дисков
* Обвал сайта
* Дезинформация

Внешние угрозы:

* Атаки со стороны информационной безопасности
* Атаки со стороны конкурентов

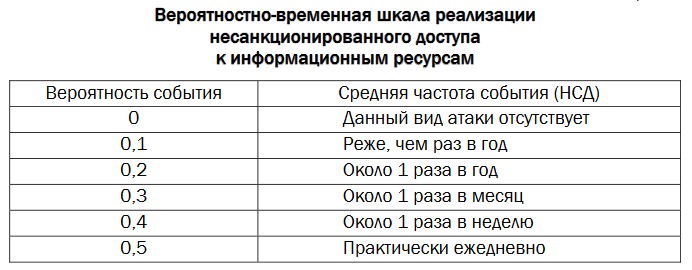
Внутренние угрозы:

* Атаки со стороны сотрудников

1. **Оценка угроз, рисков и уязвимостей.**

**Условная численная шкала для оценки ущерба компании**

|  |  |
| --- | --- |
| 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 |

****

**Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Откл. света | 1 | 0,3 | 0,3 |
| Разговоры на тему работы | 2 | 0,2 | 0,4 |
| Атаки на сервер | 3 | 0,1 | 0,3 |
| Перехват данных | 3 | 0,1 | 0,3 |
| Кража | 3 | 0,2 | 0,6 |
| Угрозы | 4 | 0,1 | 0,4 |
| Восстановление | 3 | 0,1 | 0,3 |
| Обвал сайта | 1 | 0,1 | 0,1 |
| Дезинформация | 3 | 0,1 | 0,3 |

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

* Установление норм и правил в договорах сотрудников о коммерческой тайне
* Ограничение сторонних лиц внутри офиса
* Установление камер видеонаблюдения и систем карточных пропусков
* Установка паролей и соответствующего ПО
* Установка бесперебойного оборудования на компьютеры
* Использование шифрования и защищенных сетей
* Установка безопасности на сайте
* Обеспечение безопасности сотрудникам
* 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

**Вывод:** Данное тело приобрело практические навыки разработки и внедрения эффективной политики информационной безопасности организации или учреждения.