МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 05 03 Информационные системы и технологии Направление специальности 1-40 01 05 03 Информационные системы и технологии

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №1:**

по дисциплине «Защита и надёжность информационных систем»

Тема «Разработка и внедрение политики безопасности организации или учреждения. Учреждение образования. Консалтинговая IT–компания»

Исполнитель

студентка 3 курса группы 5 Бутурля Роман Андреевич

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

*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. Таких организаций великое множество, но разбирать данную тему будем на основе консалтинговой компании.

Цели ПИБ:

* защита ресурсов
* аутентификация
* авторизация
* целостность
* конфиденциальность
* аудит безопасности

Задачами ПИБ являются:

* 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

*2. Объекты защиты. Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.*

Политика распространяется на подразделения и обязательна для исполнения всеми его сотрудниками. Положения политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

Структура управления – оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Опишем структуру консалтинговой фирмы:

1. Генеральный директор
   1. Зам директора по производству
      1. Проектный отдел
      2. Отдел маркетинга
      3. Отдел поддержки
      4. Отдел разработки
      5. Отдел внедрения
   2. Зам директора по общим вопросам
      1. Кадровая служба
      2. Юридическая служба
      3. АХЧ
   3. Главный бухгалтер
      1. Бухгалтерия

|  |
| --- |
|  |

Рисунок 1 – Схема структуры учреждения

Объекты защиты:

* документы;
* контакты сотрудников;
* сетевые каналы передачи информации.

Субъекты защиты:

* сотрудники;
* компьютеры;
* клиенты.

*3. Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.*

Основные угрозы делятся на:

* Естественные и искусственные;
* Преднамеренные и непреднамеренные;
* Внутренние и внешние.

Естественные – природные явления, не рукотворны (наводнения, пожары).

Искусственные – рукотворны (фишшинг, спам, незаконное проникновение в систему компании, незаконное проникновение в офисы компании, «Man in the middle», копирование жесткого диска из центрального офиса).

Преднамеренные – направлены на нанесение ущерба, запланированы, обдуманы (фишшинг, спам, незаконное проникновение в систему компании, незаконное проникновение в офисы компании, «Man in the middle», копирование жесткого диска из центрального офиса).

Непреднамеренные – случайное нанесение ущерба (непреднамеренное скачивание вируса).

Внутренние – ошибки, допущенные сотрудниками, или сбой оборудования, повлекшие некоторый ущерб (отказ оборудования, непреднамеренное скачивание вируса, копирование жесткого диска из центрального офиса).

Внешние – аварии, вирусы­­.

*4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты.*

При оценивании рисков учитываются:

* ценность ресурсов;
* значимость угроз и уязвимостей;
* эффективность существующих и планируемых средств защиты.

Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Таблица 1 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Спам | 1 | 0,3 | 0,3 |
| «Фишинг» | 3 | 0,2 | 0,6 |
| Вирусы | 4 | 0,2 | 0,8 |
| Недобросовестная конкуренция | 2 | 0,2 | 0,4 |
| Man in the middle | 2 | 0,2 | 0,3 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| ЧП | 4 | 0,2 | 0,8 |
| Использование незащищенных каналов для передачи данных | 2 | 0,3 | 0,6 |
| Запуск сторонних технологических программ | 2 | 0,2 | 0,4 |
| Незаконные проникновения в систему компании | 3 | 0,3 | 0,9 |
| Отказ оборудования | 2 | 0,2 | 0,4 |
| Незаконные проникновения в офисы компании | 1 | 0,2 | 0,2 |
| Итого |  |  | 6,1 |

*5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения).*

Построение надежной защиты включает оценку информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Можем выделить следующие рекомендации:

* четкая и строгая иерархия должностей и полномочий;
* строгий подбор сотрудников с привлечением;
* защита важной корпоративной почты;
* защита личных документов, отчетов в бумажном виде – копирование и перенесение информации на электронные информационные носители, защита помещения, хранящего документы;
* использование новейших средств защиты персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками.

Меры:

* спам, фишинг, вирусы, «Man in the middle» – установить ПО для защиты;
* запуск сторонних технологических программ, вирусы – проверять рабочие места сотрудников на наличие вредоносного ПО и т.п. Установить ПО для защиты;
* копирование жесткого диска из центрального офиса, незаконные проникновения в офисы компании, недобросовестная конкуренция – установить современные системы защиты в офисах компании (камеры и т.п.), усилить охрану;
* отказ оборудования – осуществлять периодическую проверку оборудования на предмет его состояния;
* незаконные проникновения в офисы компании – вести отчетность о пользователях и периодически проверять его.

*Вывод*

Приобрел практические навыки разработки и внедрения эффективной политики информационной безопасности организации или учреждения. На основе предполагаемых угроз разработана меры и требования для обеспечения внутренней безопасности.