Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**«Разработка политики информационной безопасности бизнес-компании»**

Студент: Николаева Е.В.

ФИТ 2 курс 5 группа

Преподаватель: Берников В.О.

**Практическое занятие №3**

**Введение**

Основой мер административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Определение политики ИБ должно сводиться к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

* управление доступом к средствам вычислительной техники, программа и данным;
* антивирусную защиту;
* вопросы резервного копирования;
* проведение ремонтных и восстановительных работ;
* информирование об инцидентах об области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно техническом уровнях уровне.

К процедурному уровню относятся меры безопасности, реализуемые людьми.

**Можно выделить следующие группы процедурных мер:**

* управление персоналом;
* физическая защита;
* поддержание работоспособности;
* реагирование на нарушения режима безопасности;
* планирование восстановительных работ.
  1. **Описание структуры таксопарка**

Часто руководители таксопарков жалуются на постоянную занятость. Для того чтобы быть «посвободнее» нужно уметь выстраивать командную работу. Правильная организация бизнеса позволяет выделять время на собственный отдых.

Очень часто, особенно новички бизнеса такси, думают, что кроме них решать проблемы и контролировать работу просто некому. Однако не стоит забывать о средствах автоматизации работы (контроль водителей на карте 24/7, автоматический расчет зарплаты и т.д.). В таксопарке руководитель не должен решать все проблемы, необходимо выстраивать структуру среди своих сотрудников.

**Иерархия может быть такой:**

* водитель решает вопросы с диспетчером;
* если диспетчер не решил вопрос, то водитель обращается к механику;
* если механик не смог помочь, водитель может обратиться к менеджеру (управляющему) ;
* если и управляющий не в состоянии помочь, тогда водитель должен иметь возможность обратиться напрямую к директору.

Рисунок 1 – Структура таксопарка

* 1. **Оценка рисков**

**Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации**. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы

Источники угроз по отношению к инфраструктуре таксопарка могут быть как внешними, так и внутренними.

**Источниками внутренних угроз могут являться:**

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

**Внутренние угрозы могут проявляться в следующих формах:**

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

**К внешним источникам угроз относятся**:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица: DDOS атаки, ложные вызовы;
* стихийные бедствия.

По способам воздействия на объекты информационной безопасности угрозы бывают информационные, программные, физические.

**К информационным угрозам относятся:**

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использование информации;
* использование информационного оружия.

**К программным угрозам относятся:**

* использование ошибок в ПО;
* компьютерные вирусы и вредоносные программы.

**К физическим угрозам относятся:**

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).

**Специфические угрозы безопасности:**

* возможность отключения электричества, что приведет к сбою незавершенных операций и потерям в базах данных;
* угроза передачи носителей ЭЦП и паролей к ним сотрудниками третьим лицам;
* угроза возникновения ошибок при передаче информации от других государственных учреждений;
* угроза передачи сотрудниками информации о счетах плательщика, прибыли и выручке третьим лицам;
* угроза разглашения личной информации, контактных данных, идентификационных сведений граждан, сведений о регистрации движимого и недвижимого имущества;
* угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ;
* угроза доступа в ИТ-отделе, изменения настроек сетевых параметров и потоков передачи данных между структурами;
* угроза взлома персональных страниц плательщиков в системе электронной подачи деклараций и т.д.
  1. **Разработка мер защиты**

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.

Чаще всего специалисты по безопасности:

* разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;
* проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;
* разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
* внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
* составляют планы восстановления системы на случай выхода из строя по любым причинам.

Группа технических средств защиты информации совмещает аппаратные и программные средства. Основные:

* резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;
* дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
* создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
* обеспечение возможности использовать резервные системы электропитания;
* обеспечение безопасности от пожара или повреждения оборудования водой;
* установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

**Вывод**

Важно помнить, что до внедрения каких-либо решений по защите информации необходимо разработать политику безопасности, адекватную целям и задачам организации, а также бюджету. Политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Политика информационной безопасности окажется эффективной, если она будет обеспечивать сохранение безопасности информации. При этом политику безопасности необходимо оформить в виде отдельного документа и утвердить руководством организации.