Учреждение образования “БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ”

**Практическая работа №3**

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

Выполнила:

студентка 2 курса 7 группы

Колядко Яна Дмитриевна

Проверил:

Барковский Евгений Валерьевич

ПроТТеоре

Цель: разработать проект политики информационной безопасности типографии.

**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.

## **Описание структуры типографии**

Структура полиграфических предприятий, в основном, сходна для больших, малых и средних типографий.

В структуру типографии входят генеральный директор, директор по развитию, производству, рекламе, коммерческий и финансовый директора, которым подчинены служба анализа и развития, финансовая служба и бухгалтерия, а также большое разнообразие отделов: продаж, маркетинга, рекламы, дизайна, производственный, технологический, контроля качества, снабжения, главного механика, цеха: препресс, печатный и отделочный, подразделение логистики, склад бумаги и материалов.

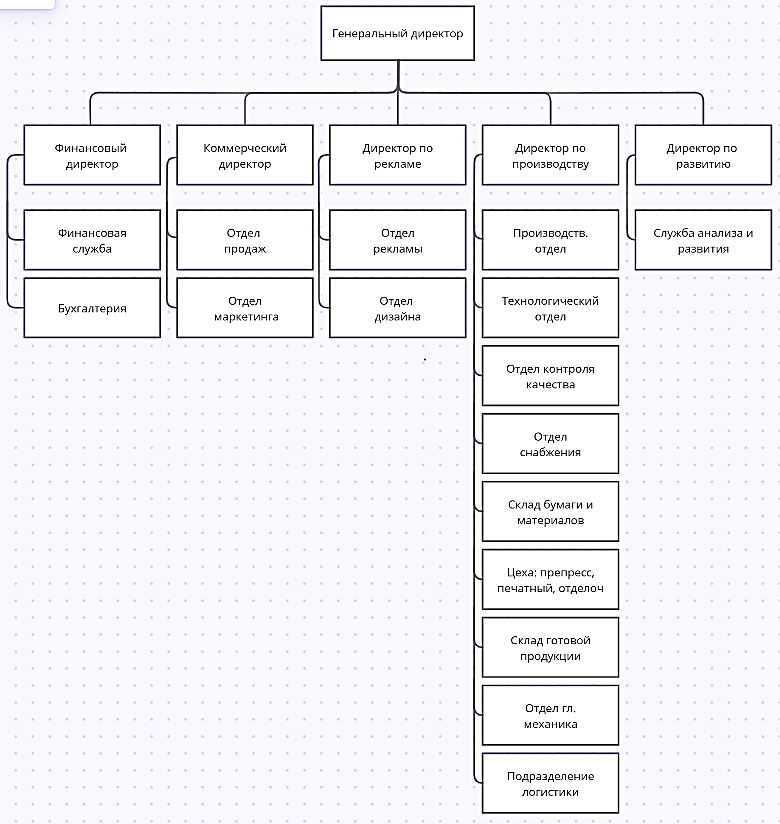


Рисунок 1 – Структура типографии

Ресурсы информационной системы, подлежащие защите:

* Данные о финансах;
* Данные и документации о недвижимости;
* Данные о клиентах;
* Нормативные документы;
* Документация о бизнес-процессах;
* Различные системы: бизнес-моделирования, бизнез-планирования, бухгалтерского учёта, обучения и тестирования персонала, информационной безопасности.

# **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 типографии могут быть как внешними, так и внутренними.

Источниками внутренних угроз могут являться:

* Сотрудники;
* 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 электронной подписи 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 взлома персональных страниц плательщиков в системе электронной подачи деклараций и т. д.

# **Разработка мер защиты**

Обеспечение информационной безопасности типографий осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты.

Физическая защита, а именно: защита зданий, сооружений и помещений.

Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов, включая:

* Защиту от вредоносного ПО;
* Резервирование серверов баз данных;
* Защиту программного обеспечения, серверов баз данных, каналов передачи информации;
* Организацию безопасного использования, преобразования, хранения и передачи информации;
* Разграничение зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников;
* Организация работы в общих программах документооборота и контроль, чтобы критически важные файлы не хранились вне сетевых дисков;
* Внедрение программных продуктов, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
* Составление планов восстановления системы на случай выхода из строя по любым причинам.

Контроль доступа, в том числе:

* Определение ответственности пользователей;
* Контроль доступа к прикладным системам.

Реализация организационно-технических мер обеспечения информационной безопасности типографий достигается при помощи:

* Корректного использования и администрирования встроенных механизмов защиты технических средств обработки, хранения и передачи информации;
* Контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по информационной безопасности;
* Резервного копирования и удаленного хранения наиболее важных блоков данных в компьютерной системе – на регулярной основе;
* Дублирования и резервирования всех подсистем сетей, которые имеют значение для сохранности данных;
* Создания возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
* Обеспечения возможности использовать резервные системы электропитания;
* Обеспечения безопасности от пожара или повреждения оборудования водой;
* Физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним.

# **Вывод**

С целью организации качественной сохранности данных следует использовать различные методы защиты информации. Начиная с охраны здания и введения пропускной системы, заканчивая ограничением доступа по уровням данным для групп пользователей. Также необходим контроль за состоянием оборудования и ПО. Не рекомендуется использовать устаревшие технические средства и программы, так как они могут привести к утечке данных из-за неисправности.

Но до внедрения каких-либо решений по защите информации необходимо разработать политику безопасности, согласно целям и задачам организации. 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 она должна быть оформлена в виде отдельного документа.