Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Защита информации и надежность информационных систем»

**Отчёт по лабораторной работе №1**

Разработка и внедрение политики безопасности типографии

Студент: Жук С.С.

ФИТ 3 курс 2 группа

Преподаватель: Савельева М.Г.

Минск 2025

**Содержание**

[Введение 3](#_Toc191980372)

[1 Объекты защиты 4](#_Toc191980373)

[1.1 Структура типографии 4](#_Toc191980374)

[1.2 Объекты информационных отношений 9](#_Toc191980375)

[1.3 Субъекты информационных отношений 10](#_Toc191980376)

[2 Основные угрозы и их источники 11](#_Toc191980377)

[2.1 Внутренние угрозы 11](#_Toc191980378)

[2.2 Внешние угрозы 11](#_Toc191980379)

[2.3 Естественные угрозы 11](#_Toc191980380)

[2.4 Искусственные угрозы 12](#_Toc191980381)

[2.4.1 Непреднамеренные угрозы 12](#_Toc191980382)

[2.4.2 Преднамеренные угрозы 12](#_Toc191980383)

[3 Оценка рисков, угроз и уязвимостей 13](#_Toc191980384)

[3.1 Оценка ущерба организации 13](#_Toc191980385)

[3.2 Оценка вероятности реализации угроз 14](#_Toc191980386)

[3.3 Оценка рисков 14](#_Toc191980387)

[4 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов 16](#_Toc191980388)

[4.1 Реализация средств защиты 16](#_Toc191980389)

[4.1.1 Нарушения в работе ПО для управления заказами 16](#_Toc191980390)

[4.1.2 Поломка основного печатного оборудования 16](#_Toc191980391)

[4.1.3 Протечка данных о клиентах 16](#_Toc191980392)

[4.1.4 Атаки на информационную систему типографии 17](#_Toc191980393)

[4.1.5 Нарушение работы системы учета материалов и запасов 17](#_Toc191980394)

[4.1.6 Невозможность выполнения заказов из-за сбоев в поставках материалов 17](#_Toc191980395)

[4.1.7 Ошибки персонала при печати или упаковке продукции 17](#_Toc191980396)

[4.1.8 Сложности с лицензированием или нарушением законодательства 18](#_Toc191980397)

[4.1.9 Пожар или наводнение в производственном помещении 18](#_Toc191980398)

[4.1.10 Падение репутации из-за плохого качества продукции или задержек 18](#_Toc191980399)

[4.2 Программа обеспечения информационной безопасности 18](#_Toc191980400)

[Заключение 20](#_Toc191980401)

# **Введение**

В современном обществе информация является одним из ключевых ресурсов, определяющих успешную деятельность организаций. В сфере полиграфии информационные потоки охватывают широкий спектр данных: от внутренних бизнес-процессов и финансовых документов до конфиденциальных заказов клиентов. Хранение, обработка и передача этих данных в электронной форме делают их уязвимыми перед различными угрозами, включая несанкционированный доступ, кибератаки и утечки информации.

В этих условиях разработка и внедрение эффективной политики информационной безопасности становятся приоритетной задачей для типографий. Политика информационной безопасности представляет собой совокупность стратегических, тактических и оперативных мер, направленных на защиту данных от потенциальных угроз, а также на обеспечение их конфиденциальности, целостности и доступности. Она является основным инструментом управления рисками в области информационной безопасности и формирует надежную основу для создания безопасной цифровой инфраструктуры типографии.

Актуальность разработки политики информационной безопасности в типографии обусловлена рядом ключевых факторов:

* зависимость от информационных технологий: современные типографии активно используют цифровые системы управления заказами, автоматизированные производственные процессы и базы данных клиентов. Потеря или компрометация этих данных может привести к сбоям в работе, финансовым потерям и ухудшению деловой репутации;
* рост киберугроз: хакерские атаки, вредоносное программное обеспечение, фишинговые атаки и утечки данных представляют серьезную опасность. Без регулярного обновления и соблюдения стандартов информационной безопасности типография становится уязвимой перед этими рисками;
* законодательные требования: соблюдение нормативных актов в области защиты информации является обязательным. Несоблюдение требований может повлечь за собой юридические последствия, штрафы и утрату доверия клиентов;
* защита конфиденциальности клиентов и партнеров: типография часто работает с конфиденциальными материалами, включая персональные данные заказчиков, корпоративные документы и эксклюзивные дизайны. Утечка или несанкционированное использование таких данных может привести к серьезным репутационным и финансовым последствиям.

Цель политики информационной безопасности – создание эффективного механизма защиты информации, минимизация рисков утечек и несанкционированного доступа, а также обеспечение соответствия законодательным требованиям. Для этого необходимо разработать четкие регламенты работы с данными, исключить потенциальные угрозы, обеспечить защиту цифровых и физических носителей информации, контролировать соблюдение мер безопасности сотрудниками. Ее внедрение позволит типографии эффективно управлять рисками, повышать надежность внутренних процессов и укреплять доверие клиентов и партнеров.

# **1 Объекты защиты**

## **Структура типографии**

Структура типографии, как важной части политики информационной безопасности, играет решающую роль в обеспечении конфиденциальности, целостности и доступности информации. Она определяет организационные процессы, правила и меры, необходимые для эффективной защиты данных и ресурсов.

Организационная структура компании представляет собой некое руководство, обеспечивающее четкое представление о том, как устроена и функционирует организация. Более конкретно, она раскрывает механизмы принятия решений в компании и определяет, кто является её руководителем.

Разработка организационной структуры предприятия является ключевой составной частью успешного управления и устойчивости бизнеса. Ниже приведены основные пункты, объясняющие необходимость разработки организационной структуры:

* распределение обязанностей и ответственности: организационная структура определяет, кто и за что отвечает в предприятии. Это позволяет установить ясные границы обязанностей и ответственности для каждого сотрудника или подразделения, предотвращая дублирование работ и конфликты интересов;
* улучшение эффективности и производительности: правильно разработанная структура помогает оптимизировать бизнес-процессы и ускорить принятие решений. Каждый сотрудник знает свою роль и место в организации, что способствует более эффективному выполнению задач;
* управление ростом и масштабирование: организационная структура должна быть спроектирована с учетом будущего роста предприятия. Она должна быть гибкой и адаптироваться к изменениям в объеме бизнеса. Это обеспечивает возможность расширения и масштабирования предприятия без серьезных сдвигов в структуре;
* упрощение управления и принятия решений: структура разделяет организацию на более мелкие и управляемые подразделения или отделы. Это делает управление более эффективным, так как руководители могут сосредотачиваться на своих функциональных областях и принимать более информированные решения;
* создание системы контроля и надзора: организационная структура позволяет установить систему контроля и надзора над деятельностью предприятия. Руководители могут отслеживать выполнение задач, оценивать результаты и вносить коррективы при необходимости;
* улучшение коммуникации и сотрудничества: организационная структура определяет пути коммуникации и сотрудничества между различными частями предприятия. Это помогает снизить вероятность информационных утечек и способствует более эффективному обмену информацией;
* соблюдение законодательства и нормативов: в зависимости от сферы деятельности, организационная структура может также помочь предприятию соблюдать законодательные требования и нормативы, предписанные регулирующими органами;
* привлечение инвестиций и клиентов: четкая и организованная структура может повысить доверие со стороны инвесторов и клиентов, что способствует привлечению капитала и расширению клиентской базы.

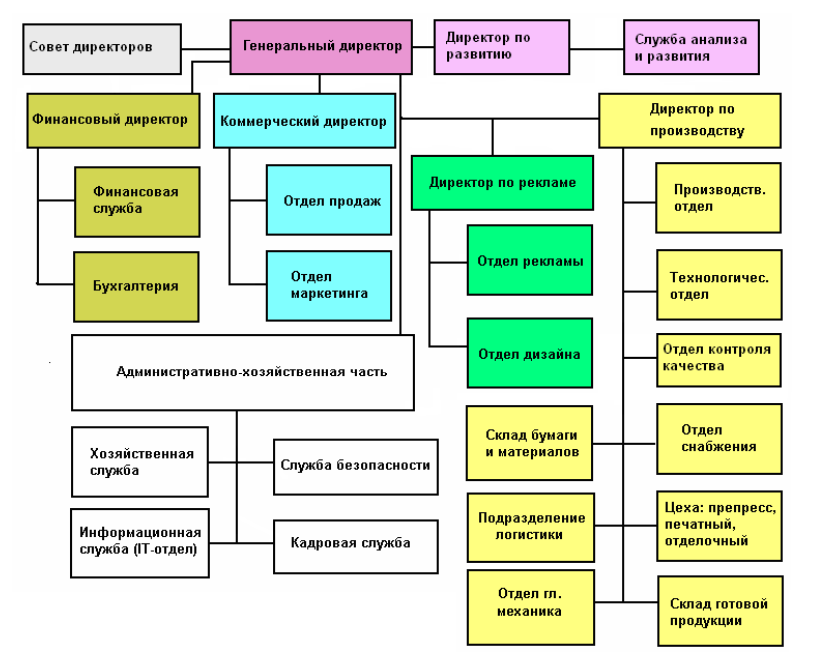


Рисунок 1.1 – Организационная структура типографии

Рассмотрим состав схемы организации типографии и функции служб и подразделений (рисунок 1.1):

1. Дирекция (служба генерального директора) осуществляет функции общекорпоративного управления. В состав дирекции входит: совет директоров, отдел развития, состоящий, например, из аналитической группы и группы информационного сопровождения.

Совет директоров – включает руководителей служб (директора по производству, административного директора, финансового директора, директора по коммерции, директора по рекламе). Взаимодействие происходит как по управленческой вертикали, так и по горизонтальным связям. Совет определяет стратегические цели и направления развития предприятия.

1. Отдел развития – выполняет анализ бизнес-процессов, сбор, обработку и анализ информации по потенциальным источникам развития предприятия. Осуществляет взаимодействие и сбор информации со всех необходимых для этих целей подразделений. Запрашивает любую необходимую внутреннюю и внешнюю информацию. Формализует и структурирует инновационно-системный потенциал предприятия. Отдел имеет непосредственные связи с генеральным директором и Дирекцией для выработки и реализации стратегии развития предприятия.
2. Административно-хозяйственная часть в общем случае состоит из четырех отделов: административно-хозяйственного отдела (группа электриков, группа сантехников, строительная группа, группа технического персонала), информационных технологий, безопасности и кадров.
3. Административно-хозяйственный отдел управляет оперативными хозяйственными мероприятиями и текущей хозяйственной деятельностью. Взаимодействие происходит практически со всеми подразделениями предприятия в области текущей хозяйственной деятельности.
4. Отдел информационных технологий обеспечивает функционирование и развитие IT-сетей предприятия, осуществляет взаимодействие со всеми отделами, где используется компьютерная техника. Участвует во внедрении новых программных и технических средств производства.
5. Отдел безопасности выполняет функции контроля за соблюдением правил и норм безопасности, для чего взаимодействует со всеми подразделениями и осуществляет различные охранные мероприятия. Совместно с отделом информационных технологий производит мониторинг и контроль входящих и исходящих информационных потоков, разрабатывает и внедряет средства по их защите.
6. Отдел кадров разрабатывает и реализует новации кадровой политики предприятия. Осуществляет взаимодействие со всеми подразделениями, имеет непосредственные связи с дирекцией и службами для выработки общекорпоративной кадровой политики.
7. Финансовая служба состоит из контрольно-ревизионного, бюджетного, аналитического отделов, а также отдела главного бухгалтера, бухгалтерии и кассы.
8. Контрольно-ревизионный отдел выполняет контроль текущих платежей, выполняет функции внутреннего аудита предприятия, для чего получает любую необходимую информацию от всех подразделений. Производит контроль подразделений касательно финансово-бухгалтерской и товарно-распорядительной документации, взаимодействует с бухгалтерией и ведет смежные участки работ с бюджетным и аналитическим отделами. Производит планово-фактический и «альтернативный» анализ. Предоставляет отчеты руководству по корректировке финансово-хозяйственной деятельности.
9. Бюджетный отдел реализует деятельность по планированию, составлению оперативных и стратегических бюджетов по подразделениям, осуществляет анализ перспективных инвестиций. Непосредственно функционально связан с бухгалтерией и аналитическим отделом. Ведет совместный планово-фактический анализ с контрольно-ревизионным отделом. Оценивает и ищет пути реализации инвестиционных решений совместно с аналитическим отделом и службой развития.
10. Аналитический отдел производит анализ финансово-хозяйственной деятельности предприятия. Взаимодействует напрямую со всеми финансовыми службами, а также осуществляет сбор необходимой информации с других подразделений в целях ведения оперативного управленческого учета и оптимизации материально-финансовых потоков. Реализует функции финансового менеджмента и инвестиционного проектирования.
11. Бухгалтерия реализует стандартные функции оперативного бухгалтерского учета текущей хозяйственной деятельности предприятия, составления различных видов бухгалтерской отчетности, ведет налоговый учет, формирует отчетность для целей управленческого учета, для чего взаимодействует со всеми подразделениями.
12. Касса осуществляет любые предусмотренные входяще-исходящие кассовые операции. Непосредственно взаимодействует с бухгалтерией и может являться одним из ее структурных подотделов.
13. Служба продаж (клиентская служба) на большинстве предприятий состоит из отделов продаж и маркетинга, а иногда и отдела связей с заказчиками.
14. Отдел продаж осуществляет клиентскую работу с заказчиками: расчет и оформление полиграфических заказов, контроль прохождения заказа в производстве, взаимодействие с заказчиком. Отдел взаимодействует со всеми клиентскими службами касательно оформления и прохождения заказов, а также предоставляет информацию в финансовые службы и дирекцию предприятия.
15. Отдел маркетинга реализует функции по сбору, обработке и анализу информации о рынке полиграфических услуг. Взаимодействует со всеми подразделениями в отношении проводимых рекламных мероприятий. Проводит анализ и позиционирование своего предприятия на рынке, а также совместные исследования с аналитическими финансовыми службами и отделом развития.
16. Отдел связей с заказчиками осуществляет контроль качественного исполнения заказов, разработку и внедрение новых схем работы с заказчиками. При этом строит свою работу на принципах прямой и обратной связей как с менеджерскими подразделениями, так и с заказчиками. Отдел контролирует правильность формализации менеджерами пожеланий заказчиков в конкретных заказах. Взаимодействует непосредственно с отделами продаж и маркетинга. Целью новых схем коммуникаций «Заказчик – Менеджер – Производство» является повышение качества и оперативности клиентского обслуживания, в том числе расширение функциональной связи с клиентом.
17. Рекламная служба состоит из двух, иногда трех подразделений – отделов рекламы, дизайна и связи с общественностью.
18. Отдел рекламы проводит анализ рынка рекламы и рекламной продукции, вырабатывает рекламную политику, осуществляет реализацию рекламных акций предприятия. Непосредственно связан с отделом маркетинга. Предоставляет необходимую информацию во все заинтересованные службы.
19. Отдел по связям с общественностью осуществляет представительские функции и формирует общественное мнение о предприятии и производимой продукции. Взаимодействует с отделами рекламы и маркетинга.
20. Отдел дизайна участвует в реализации рекламной политики, создает визуальный имидж предприятия и его тактические воплощения. Разрабатывает или заказывает и контролирует разработку рекламных материалов. Тесно взаимодействует с отделом рекламы и отделом по связям с общественностью. Согласует свою деятельность с отделом развития.
21. Производственная служба возглавляется дирекцией производства и состоит из отдела снабжения, производственного и технологического отделов, отделов главного технолога, главного механика, логистики, цехов (допечатный, печатный, брошюровочный или отделочный), складов бумаги и материалов, полуфабрикатов, готовой продукции.
22. Дирекция производства осуществляет функции общепроизводственного управления. Взаимодействует со всеми производственными подразделениями, а также предоставляет необходимую информацию в администрацию и финансовые службы. Регистрирует и нормирует технические и технологические процессы во взаимодействии со службами главного технолога и главного механика, оперативно решает производственные вопросы.
23. Производственный отдел обеспечивает диспетчеризацию и контроль прохождения заказов по технологической цепочке. Непосредственно взаимодействует с отделом продаж и производственными подразделениями (цехами). Контролирует временные и качественные показатели выполнения заказов. Предоставляет необходимую информацию в финансовые службы и отделы маркетинга и рекламы.
24. Цеха (участки) – производственные подразделения, которые реализуют технологический процесс изготовления полиграфической продукции. Взаимодействуют с дирекцией производства и представляют отчет о выполненных заказах и загруженности оборудования.
25. Технологический отдел (отдел главного технолога) осуществляет контроль за соблюдением производственных технологий, разработку и внедрение в производство новых технологий, рекомендаций для клиентской службы и отдела снабжения о возможностях применения материалов и использования новых материалов.
26. Отдел главного механика руководит ремонтом и профилактикой производственного оборудования, осуществляет связь с сервисными службами фирм – поставщиков оборудования.
27. Отдел снабжения реализует функции по снабжению производства сырьем и материалами, производит контроль остатков материалов и полуфабрикатов на складах, консультирует менеджеров о наличии материалов, возможности покупки или их замены.
28. Отдел логистики выполняет функции по выработке и организации логистических схем и потоков товародвижения как внутри, так и вне предприятия.
29. Склады непосредственно реализует функции складирования и складской оптимизации.

Основные положения, на которых строится информационная система управления типографией:

* интегрированная сетевая инфраструктура и централизованное управление: информационная система типографии должна включать в себя единую сетевую инфраструктуру и центральный контроль над разработкой информационных подсистем, нацеленных на автоматизацию ключевых задач типографии;
* обеспечение доступа ко всем информационным ресурсам типографии: информационная система должна обеспечивать доступ к всем ресурсам типографии, включая офисные приложения, дизайнерские программы, базы данных, а также средства управления производственными процессами и заказами;
* управление производственными процессами с использованием информационных ресурсов: информационная система должна поддерживать управление учебными и производственными процессами, включая планирование заказов, учет материалов и оборудования, а также контроль качества продукции;
* управление персоналом: система должна включать в себя функции управления персоналом, включая учет рабочего времени, оплату труда, а также мониторинг производительности сотрудников;
* поддержка основных бизнес-процессов и повышение их качества: информационная система должна поддерживать основные процессы типографии, такие как заказы, дизайн, печать, обработка и доставка. Она также должна способствовать повышению качества и эффективности этих процессов;
* использование современных технологий и сетевых ресурсов: для разработки, управления и сопровождения всех информационных ресурсов типографии необходимо использовать современные технологии и сетевые ресурсы. Это включает в себя использование специализированных программ и оборудования для печати и дизайна;
* поддержка информационных ресурсов для комфортной работы сотрудников и клиентов: информационная система должна обеспечивать доступ к информационным ресурсам для всех сотрудников и клиентов типографии, обеспечивая комфортное взаимодействие с системой;
* управление документооборотом: система должна поддерживать эффективное управление документами, включая хранение, поиск и передачу документов внутри и вне типографии;
* выделение необходимых ресурсов: информационная система должна гарантировать наличие достаточных ресурсов, включая вычислительные мощности, сетевую пропускную способность и хранилища данных, для обеспечения бесперебойной и эффективной работы всей типографии.

В итоге, информационная система типографии позволяет собирать, анализировать и систематизировать данные о заказах, производственных процессах и управлении персоналом, обеспечивая более эффективное и устойчивое управление бизнесом в области печати и дизайна.

## **1.2 Объекты информационных отношений**

Обеспечение безопасности и надёжности объектов информации является одной из основных задач при разработке политики информационной безопасности. В типографии можно выделить следующие объекты, требующие обеспечения информационной безопасности:

* технические и программные средства – аппаратные серверные ресурсы, лицензированное программное обеспечение, системы безопасности;
* технологическое оборудование – средства вычислительной техники, сетевое и кабельное оборудование;
* физическая инфраструктура – серверные комнаты, рабочие станции, сети передачи данных, устройства печати и сканирования;
* информационные ресурсы, в том числе содержащие сведения ограниченного распространения и представленные в виде документов в носителях на магнитной, оптической и другой основе, массивах и базах данных;
* каналы связи, передающие информацию, – кабельные и беспроводные, локальные и глобальные каналы связи.

## **1.3 Субъекты информационных отношений**

Не менее важным направлением разработки политики информационной безопасности является анализ, характеристика и разработка мер защиты субъектов информационной системы. Далее описаны субъекты, существующие в типографии:

* сотрудники организации – пользователи информационных систем, имеющие различные уровни доступа к данным в зависимости от выполняемых функций;
* руководство и владельцы бизнеса – лица, принимающие стратегические решения и ответственные за политику информационной безопасности;
* клиенты – заказчики услуг, предоставляющие персональные данные и коммерческую информацию в рамках деловых отношений;
* партнеры и поставщики – компании, обеспечивающие техническую поддержку, поставки расходных материалов и оборудования.

Таким образом, были выявлены объекты и субъекты информационных отношений.

# **2 Основные угрозы и их источники**

Главной задачей разработки политики информационной безопасности является классификация всех возможных типов потенциальных угроз, а также оценка рисков их реализации. На основании этих данных разрабатываются средства и методы для эффективного управления информационной безопасностью в типографии.

Угрозы могут быть внешними и внутренними, искусственными и естественными, а также преднамеренными и непреднамеренными. В типографии основные риски связаны с утечкой клиентской информации, несанкционированным доступом к макетам и проектам, кражей данных заказчиков, вирусными атаками, а также сбоями в оборудовании.

## **2.1 Внутренние источники угроз**

К внутренним источникам угрозам в типографии можно отнести:

* сотрудники типографии;
* разработчики программного обеспечения.

Хотя внутренние источники угроз встречаются реже благодаря современным технологиям, их последствия могут быть серьезными и приводить к финансовым потерям.

## **2.2 Внешние источники угроз**

Внешние угрозы представляют наибольший риск, так как связаны с воздействием внешних факторов, не зависящих от самой типографии. К наиболее распространенным внешним угрозам в типографии относятся:

* мошенники;
* хакеры и киберпреступники;
* природные катаклизмы;
* клиенты;

Из-за высокой вероятности реализации внешние источники угроз требуют разработки комплексной системы защиты информации в типографии.

## **2.3 Естественные угрозы**

Естественные угрозы связаны с природными и техногенными факторами, не зависящими от человека. К естественным угрозам относятся:

* перебои в электроснабжении, вызывающие сбои в работе серверов и принтеров;
* влажность и температура, влияющие на сохранность оборудования и бумажных носителей;
* электромагнитные и ионизирующие помехи, способные повредить системы хранения данных.

## **2.4 Искусственные угрозы**

Искусственные угрозы вызваны действиями человека, преднамеренными или непреднамеренными, то есть случайными. К ним относятся:

* хакерские атаки на серверы типографии с целью кражи данных клиентов и заказов;
* доступ к информации неквалифицированными сотрудниками, что может привести к искажению или утрате данных;
* распространение вирусов через внешние устройства или сети;
* ошибки персонала, ведущие к сбоям в работе оборудования.

Так как искусственные угрозы чаще всего связаны с человеческими действиями, для их предотвращения важно соблюдать строгие правила безопасности. В следующих подразделах будут рассмотрены преднамеренные и непреднамеренные угрозы.

### **2.4.1 Непреднамеренные угрозы**

Непреднамеренные угрозы возникают из-за ошибок сотрудников, случайных сбоев оборудования и неосознанных нарушений. Они могут привести к таким последствиям, как:

* потере данных из-за неправильного сохранения файлов;
* нарушению технологического процесса при печати;
* ошибкам в настройке программного обеспечения, что может привести к повреждению файлов или некорректному выполнению заказов.

Ключевой причиной таких угроз является человеческий фактор: недостаточная квалификация, стресс, невнимательность.

### **2.4.2 Преднамеренные угрозы**

Преднамеренные угрозы связаны с умышленными действиями сотрудников или сторонних лиц, направленными на нанесение ущерба компании. В типографии к таким угрозам относятся:

* кража клиентских данных и передача их конкурентам;
* взлом серверов для похищения коммерческой информации;
* умышленное уничтожение макетов, файлов или оборудования;
* халатное отношение сотрудников, приводящее к утечке данных или финансовым потерям.

Преднамеренные угрозы требуют усиленного контроля доступа к данным и внедрения системы мониторинга безопасности.

Таким образом, информационная безопасность в типографии должна учитывать все возможные угрозы –естественные, искусственные, преднамеренные и непреднамеренные. Разработка эффективной политики защиты данных поможет минимизировать риски и обеспечить бесперебойную работу предприятия.

# **3 Оценка рисков, угроз и уязвимостей**

Следующим этапом разработки политики информационной безопасности является оценка рисков. Риски можно представить как совокупность двух факторов: произведения ущерба от реализации угрозы и вероятности её реализации.

Также при оценивании рисков учитываются ценность ресурсов, значимость угроз и эффективность существующих и планируемых средств и методов защиты. Ценность ресурсов может определяться количественной или качественной характеристикой, или их комбинацией.

На основании величины рисков определяются наиболее важные и приоритетные угрозы, и на основании того, какие именно угрозы являются самыми рискованными и критически важными, определяются наиболее приоритетные меры, методы и средства защиты информационных ресурсов, а также необходимые средства управления информационной безопасностью.

То есть, для оценки рисков необходимо создать шкалу оценки ущерба типографии, вероятностно-временную шкалу реализации угрозы, которые будут рассмотрены далее.

## **3.1 Оценка ущерба организации**

Для оценки возможного ущерба типографии от реализации потенциальных угроз составляется таблица численной оценки ущерба организации, где каждой качественной степени ущерба соответствует целочисленное значение от 0 до 5. Благодаря численному ранжированию величины ущерба возможно просчитать риски на каждый тип потенциальной угрозы. Условная численная шкала оценки ущерба типографии представлена в таблице 3.1.

Таблица 3.1 – Условная численная шкала оценки ущерба типографии от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожно малый моральный и экономический ущерб типографии |
| 1 | Ущерб от атаки минимален, и положение типографии на рынке не затронуто |
| 2 | Временные финансовые потери, типография терпит убытки, но её положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные убытки или сокращение объема производства, потеря клиентов |
| 4 | Потери очень значительные, типография на период до года теряет свое положение на рынке. Для восстановления положения потребуются крупные финансовые займы |
| 5 | Типография прекращает существование |

## **3.2 Оценка вероятности реализации угроз**

Кроме того, чтобы оценить величину ущерба от реализации каждой потенциальной угрозы информационной безопасности типографии, необходимо также учитывать вероятность того, что данная угроза вообще будет реализована. Эта вероятность обусловлена следующими факторами:

* привлекательность информационных ресурсов для злоумышленников: клиентские базы данных, документы с личной информацией пользователей и сотрудников, финансовые отчётности, реализация идей и прочая информация;
* возможность использования информационного ресурса в целях получения прибыли;
* степень лёгкости, с которой угроза может быть использована;
* надёжность и безопасность существующих и планируемых систем защиты информации.

Численная классификация вероятностей реализаций различных потенциальных угроз представлена в таблице 3.2.

Таблица 3.2 – Вероятностно-временная шкала реализации угроз

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид угрозы отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

После описания численных оценок степени ущерба типографии и вероятности реализации потенциальных угроз, возможно на основании этих данных оценить риски для каждой вышеописанной потенциальной угрозы. Оценка рисков будет представлена в следующем подразделе.

## **3.3 Оценка рисков**

На основании таблиц 3.1 и 3.2 можно составить таблицу рисков. На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем. В качестве максимального допустимого уровня риска положим 1, а максимальный интегральный уровень риска примем равным 5.

Далее в каждой строке таблицы проверяется, превышает ли данная угроза предельно допустимый уровень риска или нет. Если такое превышение имеет место, данная угроза должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности.

Оценка рисков представлена в таблице 3.3.

Таблица 3.3 – Оценка рисков типографии

|  |  |  |  |
| --- | --- | --- | --- |
| Описание угрозы | Ущерб | Вероятность | Риск  (Ущерб × Вероятность) |
| Нарушения в работе программного обеспечения для управления заказами | 2 | 0,3 | 0,6 |
| Поломка основного печатного оборудования | 5 | 0,2 | 1 |
| Протечка данных о клиентах (личные данные, заказы) | 3 | 0,1 | 0,3 |
| Атаки на информационную систему типографии (вирусы, хакеры) | 4 | 0,3 | 1,2 |
| Нарушение работы системы учета материалов и запасов | 3 | 0,4 | 1,2 |
| Невозможность выполнения заказов из-за сбоев в поставках материалов | 4 | 0,2 | 0,8 |
| Ошибки персонала при печати или упаковке продукции | 2 | 0,4 | 0,8 |
| Сложности с лицензированием или нарушением законодательства | 3 | 0,1 | 0,3 |
| Пожар или наводнение в производственном помещении | 5 | 0,1 | 0,5 |
| Падение репутации из-за плохого качества продукции или задержек | 4 | 0,3 | 1,2 |
| **Итого** |  |  | **7,9** |

Согласно данным таблицы оценки рисков типографии, уровень риска для каждой угрозы не превышает допустимого предела в большинстве угроз, однако в некоторых он все же превышен. Совокупный риск от всех угроз превышает максимальное допустимое значение, равное 5. Это указывает на накопление в системе безопасности множества незначительных угроз, которые требуют комплексного подхода к их устранению. В такой ситуации приоритетными для разработки политики информационной безопасности становятся угрозы с наиболее высоким уровнем риска (1,2). Снижение вероятности их реализации или полное устранение этих угроз является ключевой задачей.

Оценка рисков для типографии является неотъемлемой частью управления бизнесом. Понимание и управление рисками помогут обеспечить устойчивое функционирование и долгосрочный успех предприятия в условиях конкурентного рынка и переменчивой экономической среды.

# **4 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Для типографии, как и для любой организации, обеспечивающей производство и обработку информации, важным шагом является внедрение эффективных методов и средств защиты данных, а также минимизация рисков, связанных с безопасностью информации. В этом разделе будут рассмотрены средства защиты, которые должны быть внедрены для снижения вероятности реализации угроз информационной безопасности или их устранения в типографии.

## **4.1 Реализация средств защиты**

Далее представлены средства защиты, которые могут быть использованы для обеспечения информационной безопасности и минимизации рисков, с которыми может столкнуться типография.

### **4.1.1 Нарушения в работе ПО для управления заказами**

Сбои в работе программного обеспечения, используемого для управления заказами, могут привести к задержкам в их выполнении, потере данных и срыву производственного процесса. Для предотвращения подобных проблем необходимо внедрение следующих мер:

* регулярное обновление программного обеспечения и резервное копирование данных;
* использование лицензированных и проверенных программных решений;
* настройка системы мониторинга с автоматическим оповещением о сбоях;
* проведение периодического тестирования и аудита программного обеспечения для выявления уязвимостей и их своевременного устранения.

### **4.1.2 Поломка основного печатного оборудования**

Поломка оборудования может привести к полной остановке производства. Для снижения рисков необходимо:

* регулярное техническое обслуживание и диагностика оборудования;
* наличие резервных запасных частей и возможность оперативного ремонта;
* заключение договоров с сервисными центрами для оперативного ремонта.

### **4.1.3 Протечка данных о клиентах**

Утечка клиентских данных может нанести серьезный ущерб репутации типографии и привести к юридическим последствиям. Для защиты данных необходимо:

* использование надежных методов шифрования при передаче и хранении данных;
* ограничение доступа сотрудников к конфиденциальной информации на основе их должностных обязанностей;
* регулярный аудит информационной безопасности;
* обучение сотрудников стандартам работы с персональными данными.

### **4.1.4 Атаки на информационную систему типографии**

Кибератаки могут привести к утечке данных, повреждению файлов и остановке работы систем. Для защиты необходимо:

* использование антивирусного ПО и межсетевых экранов;
* регулярное обновление всех программных решений;
* резервное копирование данных на защищенные носители;
* внедрение систем мониторинга подозрительной активности.

### **4.1.5 Нарушение работы системы учета материалов и запасов**

Сбои в учете материалов могут привести к дефициту или избыточному запасу сырья. Для предотвращения проблем необходимо:

* автоматизация процессов учета и использования ERP-систем;
* регулярная инвентаризация материалов и контроль запасов;
* внедрение системы предупреждения о критическом снижении запасов;
* обучение сотрудников правилам работы с учетными системами.

### **4.1.6 Невозможность выполнения заказов из-за сбоев в поставках материалов**

Задержки поставок могут привести к невыполнению заказов и потере клиентов. Для снижения риска следует:

* работа с несколькими надежными поставщиками;
* создание резерва критически важных материалов;
* заключение долгосрочных контрактов с поставщиками;
* мониторинг логистических процессов и прогнозирование потребностей.

### **4.1.7 Ошибки персонала при печати или упаковке продукции**

Человеческие ошибки могут повлиять на качество продукции и привести к убыткам. Для их минимизации необходимо:

* автоматизация процессов печати и упаковки;
* внедрение системы контроля качества на всех этапах производства;
* регулярное обучение сотрудников и тестирование их навыков;
* четкое документирование рабочих процедур и инструкций.

### **4.1.8 Сложности с лицензированием или нарушением законодательства**

Нарушение законодательных требований может привести к штрафам или приостановке деятельности. Для предотвращения этого необходимо:

* регулярный аудит юридической документации;
* контроль сроков действия лицензий и разрешений;
* обучение сотрудников требованиям нормативных актов.

### **4.1.9 Пожар или наводнение в производственном помещении**

Физические угрозы могут нанести непоправимый ущерб оборудованию и данным. Для защиты необходимо:

* установка систем пожаротушения и сигнализации;
* использование огнестойких сейфов для хранения критичных документов;
* страхование имущества типографии от стихийных бедствий;
* организация резервного копирования данных на удаленные серверы.

### **4.1.10 Падение репутации из-за плохого качества продукции или задержек**

Низкое качество продукции или несвоевременная доставка могут привести к потере клиентов. Для предотвращения подобных ситуаций следует:

* внедрение системы управления качеством;
* мониторинг обратной связи от клиентов;
* четкое планирование производства и сроков выполнения заказов;
* контроль работы сотрудников и соблюдение технологических стандартов.

## **4.2 Программа обеспечения информационной безопасности**

Информационная безопасность в типографии является важным элементом, необходимым для защиты бизнес-процессов и данных. Для того чтобы обеспечить надежную защиту информации и информационных систем, необходимо разработать комплексную программу, которая будет включать не только технические средства, но и организационные мероприятия, направленные на повышение уровня безопасности на всех уровнях предприятия.

Основные мероприятия, направленные на обеспечение информационной безопасности, должны включать несколько ключевых направлений. Во-первых, важно документировать все требования по информационной безопасности и чётко распределить обязанности среди всех сотрудников, чтобы каждый понимал свою роль в системе защиты информации. Это поможет создать основу для эффективного взаимодействия между подразделениями и обеспечения безопасности на всех этапах работы с данными.

Кроме того, необходимо проводить регулярные тренинги для сотрудников всех уровней, включая тестирование их знаний по вопросам безопасности. Обучение должно охватывать не только общие принципы защиты информации, но и конкретные процедуры, касающиеся работы с конфиденциальными данными, порядке доступа к информационным системам и механизмам защиты. Важно, чтобы сотрудники знали, как правильно обращаться с данными, какие меры предосторожности соблюдать и как действовать в случае возникновения угроз.

Ещё одним важным элементом является создание чётких инструкций по защите информации, которые должны быть разработаны и внедрены для всех сотрудников. Эти инструкции будут описывать порядок работы с конфиденциальными данными, методы защиты информации и меры по предотвращению утечек или повреждения данных.

Регулярное резервное копирование и обновление антивирусных баз являются обязательными для защиты данных от потерь и повреждений. В случае возникновения инцидентов с утечкой данных или других нарушений безопасности, типография должна иметь заранее подготовленные аварийные планы, которые описывают действия, которые должны быть предприняты в экстренных ситуациях. Эти планы должны включать не только алгоритмы восстановления данных, но и стратегию минимизации ущерба для бизнеса.

Помимо этого, важно разработать план восстановительных работ для случаев, когда угрозы безопасности реализуются. Такие планы должны регулярно тестироваться и обновляться с учётом новых угроз и изменений в инфраструктуре типографии. Это обеспечит своевременное реагирование на инциденты и позволит эффективно восстанавливать работу предприятия.

Немаловажным аспектом является физическая защита информации, которая включает организацию безопасного хранения документации и носителей данных, а также контроль доступа в помещения, где хранятся критически важные данные. Это предотвратит физическое проникновение посторонних лиц и защитит информацию от несанкционированного доступа.

Для эффективной реализации и внедрения программы обеспечения информационной безопасности необходимо разработать документацию, которая будет содержать детальное описание всех процедур и инструкций. Регулярные проверки и тестирование систем безопасности, а также контроль за выполнением этих инструкций, являются важными этапами в поддержании высокого уровня безопасности.

Важным шагом является также постоянный мониторинг и обновление политики безопасности с учётом развития технологий и появления новых угроз. Это позволит оперативно адаптироваться к изменениям внешней и внутренней среды и обеспечивать актуальность всех мер по защите информации.

Программа обеспечения информационной безопасности для типографии должна быть комплексной и многогранной, сочетая как технические средства защиты, так и организационные меры, направленные на повышение осведомленности сотрудников и улучшение процессов работы с информацией. Такой подход позволит обеспечить надежную защиту данных, минимизировать риски и сохранить репутацию предприятия на высоком уровне.

# **Заключение**

Политика безопасности – это неотъемлемая часть стратегии информационной безопасности предприятия. Она включает в себя управленческие решения, которые нацелены на защиту информации и связанных с ней ресурсов. Основной целью политики безопасности является установление технических требований и правил для обеспечения безопасности информационных систем, сетей и данных.

Важно понимать, что экономия на разработке и реализации политики безопасности может привести к серьезным последствиям, включая утечку, копирование или изменение конфиденциальных данных, что может нанести компании значительный ущерб и подороже обойтись, чем инвестиции в безопасность.

Для обеспечения информационной безопасности на предприятии необходимо применять комплексный подход, включающий технические, организационные и процессуальные меры. Это включает в себя сетевую безопасность, меры предосторожности, учет фактора человеческого фактора, обеспечение непрерывности работы и множество других аспектов.

Важно также подчеркнуть, что обеспечение информационной безопасности требует постоянной работы и обновления, поскольку угрозы постоянно меняются и развиваются. Для достижения наилучших результатов, стоит обратиться к профессиональным экспертам в области информационной безопасности, чтобы разрабатывать и внедрять меры безопасности.