ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 4](#_Toc509484751)

[АНАЛИЗ СТРУКТУРЫ ПРЕДПРИЯТИЯ С ЧЕРТЕЖОМ ОСНОВНЫХ СВЯЗЕЙ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ ПО ПОДЧИНЕННОСТИ. ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ ПОДРАЗДЕЛЕНИЙ 6](#_Toc509484752)

[КЛАССИФИКАЦИЯ ОТКРЫТОЙ И ЗАКРЫТОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ, НОСИТЕЛИ ЭТОЙ ИНФОРМАЦИИ 9](#_Toc509484753)

[ОПИСАНИЕ ОСНОВНЫХ ПУТЕЙ КОММУНИКАЦИИ, ДВИЖЕНИЯ ИНФОРМАЦИИ 11](#_Toc509484754)

[ХАРАКТЕРИСТИКА ИС НА ПРИКЛАДНОМ УРОВНЕ. 12](#_Toc509484755)

[ХАРАКТЕРИСТИКА ИС НА СИСТЕМНО-ТЕХНИЧЕСКОМ УРОВНЕ 14](#_Toc509484756)

[РАЗРАБОТКА МОДЕЛИ УГРОЗ ИС, ОБРАБАТЫВАЮЩИХ КИ 21](#_Toc509484757)

[ОБОСНОВАНИЕ НЕОБХОДИМОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ КТ 27](#_Toc509484758)

[АНАЛИЗ ОСНОВНЫХ ПУТЕЙ УТЕЧКИ ИНФОРМАЦИИ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 30](#_Toc509484759)

[РАЗРАБОТКА СТРУКТУРЫ СЛУЖБЫ БЕЗОПАСНОСТИ С ОПИСАНИЕМ ОСНОВНЫХ ФУНКЦИЙ ПОДРАЗДЕЛЕНИЙ 34](#_Toc509484760)

[ПЛАН ТЕРРИТОРИИ ПРЕДПРИЯТИЯ ИЛИ ПОЭТАЖНЫЕ ПЛАНЫ С ВЫДЕЛЕНИЕМ И ОБОЗНАЧЕНИЕМ ЗОН БЕЗОПАСНОСТИ, А ТАКЖЕ ПУТЕЙ ПРОХОДА В ЭТИ ЗОНЫ 38](#_Toc509484761)

[РАЗРАБОТКА ДОЛЖНОСТНЫХ ИНСТРУКЦИЙ СОТРУДНИКОВ СЛУЖБЫ БЕЗОПАСНОСТИ 39](#_Toc509484762)

[РАЗРАБОТКА ДОКУМЕНТА «ПОЛИТИКА ИБ ОРГАНИЗАЦИИ» 52](#_Toc509484763)

[ЗАКЛЮЧЕНИЕ 59](#_Toc509484764)

[СПИСОК ЛИТЕРАТУРЫ 60](#_Toc509484765)

# ВВЕДЕНИЕ

На предприятии разрабатываются чертежи, схемы, разнообразное техническое оборудование, программное обеспечение, документация. Потеря или утечка такой информации может привести к очень большим убыткам на предприятии. В связи с этим, всю информацию предприятия необходимо защищать. Организация защиты объектов информатизации подразумевает регламентацию всей деятельности предприятия таким образом, чтобы исключить или свести к минимуму уязвимость объектов к внешним и внутренним угрозам.  
 На данный момент одной из самых распространенных автоматизированных систем защиты объектов является система контроля и управления доступом – СКУД.

Целью курсового проекта является организация защиты вымышленного предприятия АО «Ласточка», основными видами деятельности которого являются конструирование технического оборудования и разработка программного обеспечения для них. Помещение занимает один этаж офисного здания.

Для выполнения поставленной цели необходимо выполнить следующие задачи:

* составить перечень информационных систем в организации, занимающихся обработкой конфиденциальной информации;
* составить перечень участвующего в процессе деятельности серверного и сетевого оборудования;
* определить и проанализировать основные пути утечки и угроз информационной безопасности;
* определить набор используемого программного обеспечения и средств защиты информации от несанкционированного доступа, включающие в себя межсетевые экраны, антивирусные средства и т.д.;
* организовать защиту территории предприятия с использования систем контроля и управлением доступом, а также разработать документ, описывающий политику информационной безопасности предприятия.

# АНАЛИЗ СТРУКТУРЫ ПРЕДПРИЯТИЯ С ЧЕРТЕЖОМ ОСНОВНЫХ СВЯЗЕЙ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ ПО ПОДЧИНЕННОСТИ. ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ ПОДРАЗДЕЛЕНИЙ

Под предприятием понимается любой объект, обрабатывающий материальные или информационные потоки. Оно включает в себя здания и прилегающие к ним территории, границы которой могут быть обозначены физической преградой или просто зафиксированы законодательно.

Предприятие включает в себя помещения и участки различного назначения, в том числе:

* кабинет руководящего состава и совещательные комнаты;
* кабинеты сотрудников и основных служб;
* представительские и переговорные помещения;
* помещения технических служб, а именно: узлы энергоснабжения, водоснабжения, газоснабжения, телефонный узел, склады и т.д.;
* производственные помещения с оборудованием;
* хранилища ценностей, оружия, вредных и опасных веществ;
* хранилища различных носителей информации.

Для защиты предприятия необходимо составить его структуру.

Во главе АО «Ласточка» находится генеральный директор, которому подчиняются остальные руководители отделов.

Коммерческий директор ответственен за отделы, занимающиеся снабжением предприятия, логистикой и сбытом продукции.

Финансовый директор контролирует финансовую деятельность предприятия, которая включает составление финансовых отчетов и планов на экономическое развитие предприятия.

Технический директор контролирует отделы, занимающиеся разработкой продукции предприятия. Сюда включены отдел по разработке ПО, отдел научно-исследовательских работ и отдел опытно-конструкторских работ.

Директор по персоналу ответственен за подбор кадров и контроль за персоналом на предприятии. Начальник службы безопасности ответственен за полную защиту предприятия, включая информационную и физическую.

Структура предприятия АО «Ласточка» представлена на рисунке 1.

Структура предприятия, рис.1



# КЛАССИФИКАЦИЯ ОТКРЫТОЙ И ЗАКРЫТОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ, НОСИТЕЛИ ЭТОЙ ИНФОРМАЦИИ

Из-за циркуляции большого количества информации, ее нужно защищать различными средствами. В связи с этим всю информацию необходимо классифицировать.

Информация бывает открытая и закрытая.

Открытую информацию необходимо защищать, обеспечивая защиту целостности для предотвращения её фальсификации, однако требования к конфиденциальности к ней не применяются.

В нашем случае, открытой информацией будет являться:

* цены продукции;
* качество продукции;
* финансовая или бухгалтерская отчетность.

К закрытой информации в дополнение к целостности и доступности, предъявляются требования конфиденциальности.

Закрытая информация включает в себя конфиденциальную информацию и информацию для внутреннего использования.

На рассматриваемом предприятии конфиденциальную информацию составляют коммерческая тайна и персональные данные работников предприятия. Предприятие АО «Ласточка» занимается конструированием разнообразного технического оборудования.

Для данного предприятия коммерческая тайна включает:

* чертежи и схематику разрабатываемых устройств;
* разрабатываемый код;
* концепты продукции;
* коммерческие договоры.

Информация для внутреннего пользования тоже подлежит защите. Она необходима для работоспособности предприятия, однако её утечка окажет не настолько серьёзное воздействие на предприятия, как коммерческая тайна. Включает:

* данные по организации безопасности;
* планы работ;
* содержание бухгалтерского учета

# ОПИСАНИЕ ОСНОВНЫХ ПУТЕЙ КОММУНИКАЦИИ, ДВИЖЕНИЯ ИНФОРМАЦИИ

Информационные потоки отражают перемещение информации внутри предприятия от одного отдела к другому или общение внутренних отделов с внешними объектами.

Составлять схемы потоков необходимо для оптимизации работы предприятия.

Внешние информационные потоки

|  |  |  |
| --- | --- | --- |
| **Отправитель** | **Получатель** | **Вид передаваемой информации** |
| Коммерческий отдел | Рынок | Открытая |
| Отдел кадров | Люди, которые ищут работу | Открытая |
| Проектно- конструкторский отдел | Производственный отдел | Закрытая |
| Коммерческий отдел | Поставщики | Закрытая |
| Бухгалтерия | Налоговая служба | Закрытая |

Внутренние информационные потоки

|  |  |  |
| --- | --- | --- |
| **Отправитель (Получатель)** | **Получатель (Отправитель)** | **Вид передаваемой информации** |
| Генеральный директор | Финансовый директор | Закрытая |
| Генеральный директор | Директор по персоналу | Закрытая |
| Генеральный директор | Начальник службы безопасности | Закрытая |
| Бухгалтерия | Коммерческий директор | Закрытая |
| Бухгалтерия | Генеральный директор | Закрытая |
| Генеральный директор | Коммерческий директор | Закрытая |
| Коммерческий директор | Проектно- конструкторский отдел | Закрытая |

# ХАРАКТЕРИСТИКА ИС НА ПРИКЛАДНОМ УРОВНЕ.

Система контроля и управления доступом (СКУД) «Сторк» позволяет организовать контроль доступа в помещение.

Система включает в себя: серверы оборудования, автоматизированное рабочее место (АРМ) с индивидуальной конфигурацией, которая может включать сервер лицензий, конфигуратор системы, генератор отчетов, учет рабочего времени, модуль фото-видеоверификации и пр. Интегрированная система рассчитана на работу с исполнительными устройствами типа шлагбаумов, ворот, турникетов, калиток, электромеханических (электромагнитных) замков, сирен, строб-вспышок, охранных датчиков сигнализации, бесконтактных считывателей.

СКУД Stork работает с системой видеонаблюдения «Линия».

Основной целью интеграции двух систем является повышение уровня безопасности на охраняемых объектах за счет быстрого реагирования элементов систем, актуального информирования об инцидентах, упрощенного управления новыми доступными приложениями.

Плюсом совместной работы СКУД Stork с системой IP-видеонаблюдения «Линия» также является сокращение эксплуатационных затрат. Обе системы могут быть установлены на 1 ПК, который может служить одновременно сервером для хранения и передачи данных и рабочим местом сотрудника охранного подразделения. Экономия ресурсов ПК обусловлена тем, что все реакции систем реализуются в одном интерфейсе - интерфейсе СКУД Stork.

Масштабируемость обеих систем дает возможность наращивания элементов до необходимого количества.

Так же компания Сторк предлагает программное обеспечение «StorkAccess»

Классический функционал общий для всех — конфигурация контроллеров, наблюдение в режиме реального времени за событиями происходящими в системе, настройка прав пользователей, создание карточек персонала, редактор шаблонов пропусков, учет рабочего времени, графические планы, фотоверификация, sms и е-mail оповещения.

# ХАРАКТЕРИСТИКА ИС НА СИСТЕМНО-ТЕХНИЧЕСКОМ УРОВНЕ

Основные технические характеристики

Автономный контролер СКУД LC-1DW

|  |  |
| --- | --- |
| Количество пользователей | В системе - неограниченно, 1 контроллер - до 900 |
| Интерфейс подключения считывателя | Wiegand 26, Dallas TM. |
| Управление | Подключение и управление всеми типами замков |
| Количество используемых мастер-ключей | 2 |
| защита кода жетона | 5 байтная |
| Количество подключаемых кнопок | 1 |
| Возможность переноса базы пользователей в сетевую версию СКУД | Есть |

Программное обеспечение «StorkAccess».

1. ОБЩИЕ СВЕДЕНИЯ

Система контроля и управления доступом (далее СКУД) предназначена для фиксации и управления перемещениями людей в помещениях и на территории охраняемого объекта. Всем сотрудникам компании, где установлена СКУД, выдаются электронные пропуска (пластиковые карты или брелоки), содержащие персональные коды доступа. На основании этих кодов и информации о владельце, хранящейся в базе данных СКУД система принимает решение о разрешении или запрете прохода на территорию объекта.

2. СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Программное обеспечение StorkAccess (далее ПО) является сетевой версией, которая подразумевает работу по управлению доступом с одного или нескольких персональных компьютеров, объединенных в единую локальную сеть, и состоит из следующих компонентов:

**СУБД (Система Управления Базами Данных)** – Firebird-2.5.2.26539 (Classic Server) 32/64-bit или новее.

**База данных СКУД (SKD\_STORK.FDB)** – предназначена для хранения, обработки и анализа информации о происходящих на защищаемом объекте событиях. Путь – C:\Program Files\StorK\FireBird\data\SKD\_STORK.FDB.

**Менеджер оборудования** - обеспечивает взаимодействие сетевых контроллеров с базой данных СКУД, по средствам преобразователей интерфейсов (конвертеров) RS232/RS-485 или USB/RS-485 компании Stork. Представлен в виде отдельного приложения или службы Windows (выбирается при установке ПО).

**СторК - сервер ключа** **(StorkKey.exe)** – Служба Windows , которая обеспечивает управление лицензиями клиентского программного обеспечения (StorkManager) и менеджеров оборудования.

**Автоматизированное рабочее место оператора (StorkManager.exe)** – клиентское ПО, для контроля и управления системой СКУД. Взаимодействует непосредственно с базой данных СКУД.

**Утилита создания резервных копий базы данных.**

**Утилита восстановления базы данных.**

**Служба оповещений.** Предназначена для информирования пользователей о работе комплекса СКУД по электронной почте (E-Mail) или SMS.

3. ТРЕБОВАНИЯ К РАБОЧИМ МЕСТАМ

Рабочие места должны удовлетворять следующим требованиям:

СанПиН 2.2.1/2.1.1.1278-03 - Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий.

СанПиН 2.2.2.1332-03 - Гигиенические требования к организации работы на копировально-множительной технике.

СанПиН 2.2.2/2.4.1340-03 - Гигиенические требования к персональным электронно- вычислительным машинам и организации работы.

СанПиН 2.2.3.1385-03 - Гигиенические требования к предприятиям производства строительных материалов и конструкций.

4. ПРОГРАММНО-АППАРАТНЫЕ ТРЕБОВАНИЯ

Программный комплекс StorkAccess может быть установлен как на отдельном персональном компьютере, так и на разных компьютерах объединенных локальной сетью.

Установка StorkAccess на отдельном персональном компьютере предпочтительна в тех случаях, когда объем обрабатываемой информации комплексом СКУД является не значительным, например, в небольших офисах с малым количеством сотрудников, а для работы с системой достаточно одного рабочего места оператора.

Установка StorkAccess на разных компьютерах предпочтительна в относительно крупных офисных комплексах. Для развертывания комплекса СКУД могут быть задействованы в данном случае уже функционирующие персональные компьютеры или сервера.

5. АППАРАТНЫЕ ТРЕБОВАНИЯ

5.1.1 Серверное оборудование

База данных является основным компонентом системы СКУД. И как в любой СУБД, на производительность влияют: количество памяти, скорость работы дисковой подсистемы, и т. д. Рекомендации для выбора аппаратного обеспечения зависят от требований к системе, прогнозируемого размера базы данных, количества пользователей (сотрудников), и т.д. Допустимо начинать с минимальной конфигурации, расширяя её по мере надобности. Для нормального функционирования СУБД необходимо серверное оборудование или персональные компьютеры, удовлетворяющее следующим требованиям:

CPU (процессор) на базе семейств Intel или AMD с частотой не менее 2 ГГц (рекомендуется Intel Core2Duo), 32-х или 64-х разрядный.

RAM (оперативная память) не менее 2 Гб (рекомендуется 4 Гб).

HDD (жесткий диск). Рекомендуется использовать два жестких диска, один под операционную систему, другой под базу данных и хранилище архивных копий. Объем первого диска должен составлять не менее 80 Гб. Объем второго диска - 160 Гб (рекомендуется 320 Гб или более). В случае использования одного жесткого диска его емкость должна составлять не менее 160 Гб. Жесткий диск должен содержать два раздела со следующим процентным соотношением: основной раздел (операционная система) – 20% от общего объема диска, раздел D (база данных и хранилище): – 80%.

Наличие на материнской плате штатных СОМ-портов в случае подключения линии связи (RS-485) к персональному компьютеру с использованием конвертера RS-232/485. В случае отсутствия штатных COM-портов допускается использование PCI-плат расширения COM-портов.

Наличие свободных USB-портов в случае подключения линии связи с использованием преобразователя интерфейсов USB/RS-485.

Наличие сетевого адаптера с установленным и настроенным протоколом TCP/IP со скоростью передачи не менее 100 Мбит/сек.

Наличие источника бесперебойного питания UPS с управляющим программным обеспечением для корректного завершения работы ПО и базы данных СКУД в том случае, если внешнее питание не будет восстановлено в течение максимального времени работы ИБП от батарей.

5.1.2 Клиентское оборудование

Клиентский компьютер используется для размещения АРМ-ов системы СКУД или серверов оборудования и должен удовлетворять следующим требованиям:

CPU (процессор) на базе семейств Intel® или AMD с частотой не менее 1 ГГц (рекомендуется 2 ГГц).

RAM (оперативная память) не менее 1 Гб (рекомендуется 2 Гб).

HDD (жесткий диск). Для установки клиентского программного обеспечения на жестком диске должно быть не менее 100 Мбайт свободного дискового пространства.

Наличие сетевого адаптера с установленным и настроенным протоколом TCP/IP со скоростью передачи не менее 100 Мбит/сек.

Наличие в материнской плате штатного СОМ-порта для подключения настольного считывателя FlyRS232. В случае отсутствия штатного COM-порта возможно использование PCI-плат расширения COM-портов.

Наличие свободного USB-порта, для подключения настольного считывателя USBFlyRS. Настольные считыватели служат для занесения жетонов сотрудников в базу данных системы.

Видеокарта и монитор с разрешением не менее 1024х768 точек и глубиной цвета не менее 32bit.

Звуковая карта для выдачи тревожных сообщений при их активации в разделе "Справочник событий".

Клавиатура.

Манипулятор "мышь".

Коврик для мыши.

Наличие источника бесперебойного питания UPS

При установке StorkAccess на отдельном персональном компьютере данный компьютер одновременно будет являться сервером и клиентским компьютером, поэтому он должен соответствовать требованиям, предъявляемым к серверу.

5.2 Программные требования

Работоспособность ПО тестировалось на следующих операционных системах:

Windows 2000 Server или Professional + Service Packs 4

Windows 2003 Server (Standard Edition, Enterprise Edition) + Service Packs 2

Windows XP (все виды)

Windows 7 (все виды)

Windows Server 2008 (все виды)

Windows 8 или 8.1 (все виды)

Для полноценной работы программного обеспечения требуется наличие дополнительного программного обеспечения:

Microsoft Internet Explorer 8 или выше, для отображения справочной информации (в поставку не входит).

Microsoft Office начиная с версии 2003 или новее, для возможности выгрузки отчетов модуля трудовой дисциплины в Word или Excel (в поставку не входит).

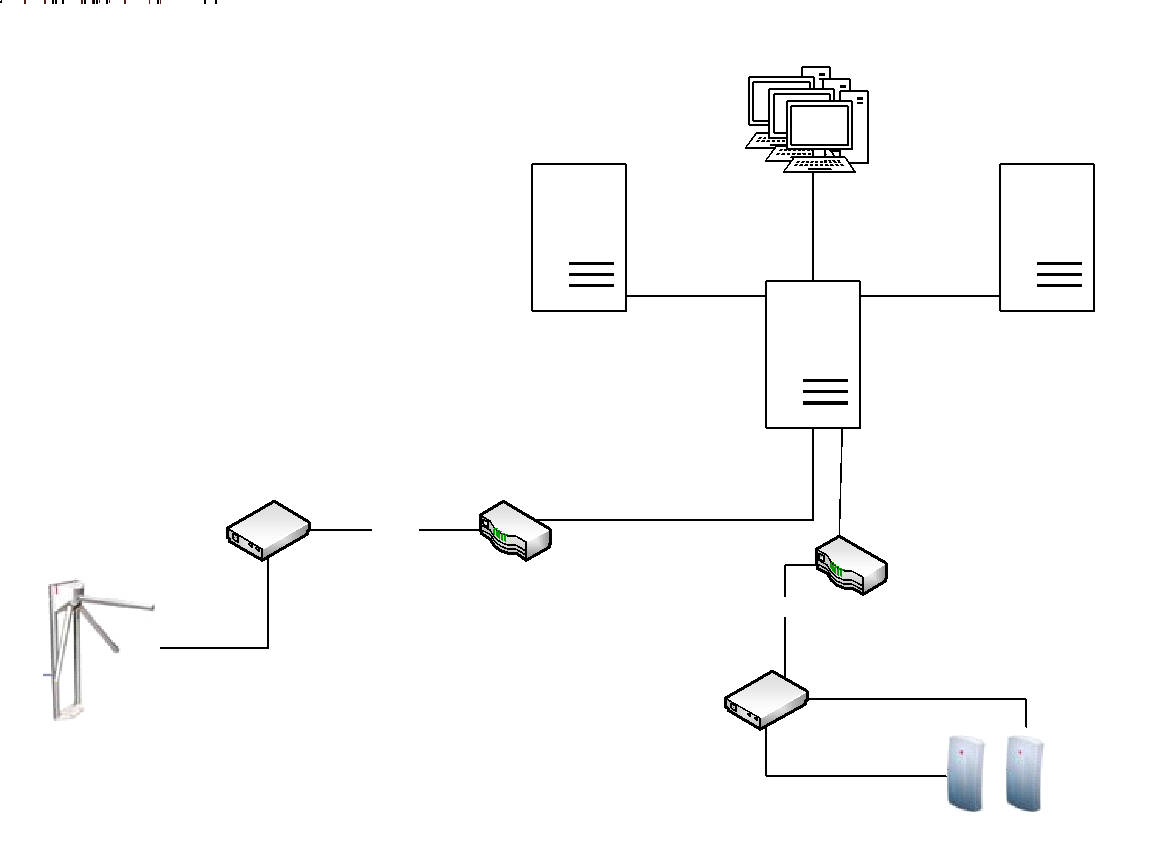


Схема построения системы.

# РАЗРАБОТКА МОДЕЛИ УГРОЗ ИС, ОБРАБАТЫВАЮЩИХ КИ

Для системы контроля и управлением доступа главной угрозой является человеческий фактор.

В целом личность нарушителя можно определить как личность человека, который способен на преступления вследствие присущих ему психологических особенностей, антиобщественных взглядов, отрицательного отношения к нравственным ценностям и вследствие выбора общественно опасного пути для добровольного удовлетворения своих потребностей, под принуждением или в силу сложившихся обстоятельств.

Тип нарушителя характеризует его отношение к защищаемому объекту и его возможности по преодолению системы охраны.

1. Типология нарушителей по подготовленности к преодолению системы охраны.

Специалист. К этой категории можно отнести людей, профессионально занимающихся данным видом деятельности и имеющих специальную подготовку. Они могут действовать в интересах конкурентов или преследовать личные цели.

Любитель. К этой категории относятся наемники или люди, остро нуждающиеся в средствах (например, безработные), обдуманно совершающие противоправные действия.

Дилетант. Можно отнести хулиганов, наркоманов, алкоголиков, совершающих проникновение без предварительной подготовки. Они преследуют, как правило, корыстные цели или мелкое вредительство.

Сотрудник - это человек, работающий непосредственно на объекте защиты, его цель - обогащение.

1. Типология нарушителей по характеру поведения.

В целом личность нарушителя можно определить как личность человека, который идет на совершение преступления вследствие присущих ему психологических особенностей, антиобщественных взглядов, отрицательного отношения к нравственным ценностям и вследствие выбора общественно опасного пути для удовлетворения своих потребностей или непроявления необходимой активности в предотвращении отрицательного результата.

Специфическая сущность личности нарушителя заключается в особенностях его психического склада, которые выражают собой внутренние предпосылки антиобщественного поведения Общественная опасность выражает потенцию личности к преступному поведению, которая понимается как внутренняя возможность совершения при определенных условиях преступных действий.

Можно выделить две группы нарушителей, отличающихся характером поведения при совершении противоправных действий на объекте, -осторожные и неосторожные.

Осторожные нарушители характеризуются:

* низким уровнем тревожности;
* проявляют общительность, стремятся к установлению межличностных контактов;
* социально адаптированы;
* в наименьшей степени упрекают себя за совершение преступления.

Неосторожные нарушители характеризуются:

* высоким уровнем тревожности;
* отличаются интрапунитивными реакциями в ситуации фрустрации (возложение ответственности за неудачи на себя) в отличие от умышленных преступников, для которых свойственны экстрапунитивные реакции (склонность во всем винить окружающих людей);
* проявляют неуверенность в себе, склонность к волнениям при стрессе, избыточный самоконтроль, дезорганизованное поведение;
* реализуют эмоциональные, а не рациональные, спокойные реакции на угрозы в экстремальной ситуации;
* создают в максимальной степени аварийные ситуации в состоянии алкогольного опьянения при управлении транспортным средством.

1. Типология нарушителей-террористов.

Отдельное место среди правонарушителей занимают террористы.

В наиболее обобщенном виде в можно выделить три психологические модели личности террориста:

* Психопат-фанатик.

Этот тип террористов руководствуется своими убеждениями (религиозными, идеологическими, политическими) и искренне считает, что его действия, независимо от их конкретных результатов, полезны для общества. У психопата-фанатика сфера сознания крайне сужена какими-либо доктринами, им же подчинена эмоциональная сфера. Если мотивы его действий носят объективно антиобщественный характер, то он способен совершить большие злодеяния.

* Фрустрированный человек.

Чувство фрустрации, порожденное невозможностью для человека по каким-то причинам достичь жизненно важных для него целей, неизбежно порождает у него тенденцию к агрессивным действиям. Сознание в этом случае может сыграть роль инструмента в рационализации этих действий, то есть в подборе тех или иных поводов для их оправдания.

* Человек из ущербной семьи.

Жестокое обращение родителей с ребенком, его социальная изоляция, дефицит добрых отношений могут привести к формированию озлобленной личности с антисоциальными наклонностями. При определенных условиях люди такого психологического склада легко могут стать инструментами террористической организации.

5. Типы криминогенности личности.

Описанные психологические особенности нарушителей следует рассматривать как предрасположенность к совершению преступления, то есть как систему свойств индивида, понижающую криминогенный порог. Однако реализация этой предрасположенности, генезис преступного поведения зависят от направленности личности, ее ценностных ориентации, складывающихся под влиянием социальных отношений, в которые был включен индивид.

Генезис преступного поведения заключается в формировании у индивида состояния психологической готовности к поведенческому акту в форме противоправныхдействий. Центральным моментом здесь является принятие криминальной цели и способа, в специфике которого проявляются наиболее существенные психологические особенности личности. Это позволяет выделить ряд общих типов криминогенности личности:

* первый тип характеризуется тем, что готовность к совершению преступного деяния обусловливается наличием определенной криминальной потребности, предметом которой является не только получаемый результат, но и сами преступные действия - процесс их совершения;
* второй тип выражается в субъективно непротиворечивом принятии преступного способа удовлетворения некоторой потребности или разрешения проблемной ситуации как наиболее предпочтительного по сравнению с правомерным или наряду с использованием правомерного;
* третий тип выражается в том, что субъект принимает преступный способ удовлетворения определенной потребности лишь при исключительно благоприятных условиях, которые предоставляют не только достаточную возможность получения личностно ценного результата преступным способом, но и максимальную безопасность;
* четвертый тип проявляется в вынужденном, внутренне противоречивом принятии преступного способа действий;
* пятый тип характеризуется наличием склонности к импульсивному совершению противозаконных действий, проявляемой в форме реакции на некоторые обстоятельства ситуации;
* шестой психологический тип проявляется в принятии преступной цели-способа под решающим влиянием внешнего криминогенного воздействия иных лиц либо в результате его конформного поведения в группе, обусловленного готовностью идентифицировать с ней свое поведение.

5. Типология нарушителей по физической и технической подготовленности.

Физическая подготовленность нарушителя характеризуется развитостью его физических возможностей по перемещению на объекте, преодолению препятствий.

Объединяя психологические особенности и физическое состояние можно охарактеризовать вы-сокоподготовленного нарушителя как осторожного, решительного, физически развитого человека. Слабый уровень психофизической подготовленности характеризуются плохим физическим развитием, высоким уровнем тревожности нарушителя, неуверенностью в себе. Между ними промежуточное положение занимает средний уровень психофизической подготовленности.

Уровень технической подготовленности нарушителя характеризуется наличием специальных технических средств для проникновения и навыками в обращении с ними. Высокая степень технической подготовленности характеризуется наличием специального набора инструментов, оборудования и высокой квалификацией нарушителя по их применению. Для технически среднеподготовленного внешнего или внутреннего нарушителя это может быть подобранный под задачу наборсамодельных или усовершенствованных технических средств. Нарушитель с низким уровнем технической подготовки использует подручные, бытовые легкодоступные средства или не использует их вообще.

6. Типология нарушителей по осведомленности об объекте.

Осведомленность нарушителя об объекте и системе охраны на нем существенно влияет на уровень его подготовленности. Можно выделить три следующих уровня осведомленности:

* высокая - нарушитель знает практически все об объекте и системе охраны, их уязвимых местах;
* средняя - нарушитель знает сравнительно много об объекте, но не знает его уязвимых мест, недостаточно знаний о системе охраны, значимости критических элементов объекта и точных местах их нахождения;
* низкая - нарушитель имеет общее представление о назначении объекта и системе его физической защиты, но практически ничего не знает об уязвимых местах объекта, значимости и местах нахождения его критических элементов.

# ОБОСНОВАНИЕ НЕОБХОДИМОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ КТ

Коммерческая тайна - режим конфиденциальности информации, позволяющей ее обладателю при существующих обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Предприятие может обеспечить юридическую защиту своих сведений, составляющих коммерческую ценность только в случае установления на предприятии режима коммерческой тайны и проведения всех необходимых мероприятий по обеспечению защиты информации. Если такой режим не введен, то это означает, что компания не предприняла необходимых действий для защиты собственных секретов и не может претендовать на юридическую защиту собственных интересов со стороны государства.

Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Система защиты коммерческой тайны создаётся в целях:

- достижения устойчивых позиций в условии конкурентной борьбы на рынке товаров и услуг;

- сохранения конфиденциальной информации в течение определённого промежутка времени;

- получения возможности проверить каждый из вероятных каналов утечки информации;

- предотвращения негативных последствий текучести кадров.

К разряду коммерческой тайны относятся следующие данные: 1) Научно-техническая информация – включает открытия, идеи, патенты, ноу-хау, новые методы организации производства, лицензии, планы внедрения новых технологий и прочих видов продукции, программное обеспечение, анализ конкурентоспособности продукта, пароли доступа к конфиденциальным данным; 2) Производственная информация. В том числе данные о способах производства, технологии, схемы, чертежи, конструкторские документы, рецептура товаров, информация о материалах, время выхода на рынок, производственные и инвестиционные планы; 3) Финансовые данные – себестоимость товара, размер прибыли, торговые, банковские операции, механизм формирования цен, платежеспособность компании; 4) Деловая информация – условия и характер заключенных контрактов, данные о поставщиках, планы проведения рекламных акций, сведения о коммерческой переписке, деловых переговорах.

Злоумышленники при хищении коммерческой тайны преследуют, как правило, 3 цели:

1. Получение необходимых сведений в объеме, которого достаточно для успешной конкурентной борьбы;

2. Нанесение ущерба для конкурента, уничтожая его ценную информацию;

3. Внесение изменений в информационные потоки компании-конкурента, преследуя свои цели и интересы.

Основная цель функционирования системы защиты информации – установить оптимальный режим работы предприятия с таким расчетом, чтобы ограничить распространение сведений, содержащих коммерческую тайну, сделать эти сведения недоступными для посторонних лиц, предотвратить их утечку и создать необходимые условия работы лицам, имеющим к ним законный доступ.

Система защиты коммерческой тайны требует комплексного подхода и включает в себя различные направления.

- Законодательная защита – соблюдение прав предпринимателя на конфиденциальные данные, закрепленных российским законодательством.

- Физическая защита — организация пропускного режима на предприятии, охраны, введение специальных карточек для посторонних, работа с закрывающимися шкафами, сейфами и пр.

- Организационная защита:

1. Создание службы либо введение должности, ответственной за отнесение информации к разряду коммерческой тайны, следование правилам доступа и использования информации;

2. Соблюдение правил пользования информацией, постоянно действующая система контроля соблюдения правил доступа, пользования информацией;

3. Разделение информации по степени конфиденциальности. Допуск к коммерческой тайне организуется лишь в соответствии с уполномоченной должностью либо с разрешения руководства компании.

- Техническая защита – используются средства контроля и защиты, в том числе сигнализирующие устройства, микрофоны, видеокамеры, средства идентификации, программные средства защиты компьютерных систем от попыток несанкционированного доступа.

- Работа с кадрами – активная работа кадровых служб компании по набору, обучению, проверке, продвижению, расстановке, стимулированию и продвижению персонала. Необходим регулярный инструктаж сотрудников о важности следовать правилам пользования данными коммерческой тайны, донося информацию об ответственности по факту нарушения.

# АНАЛИЗ ОСНОВНЫХ ПУТЕЙ УТЕЧКИ ИНФОРМАЦИИ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аналитический центр InfoWatch опубликовал данные по утечке данных в России за 2017 год. Согласно исследованию, СМИ обнародовали 213 случаев утечек информации из российских госорганов и компаний, что составляет 14% от общемирового количества утечек.

Самые частые случаи — это утечка платежной информации и персональных данных — 80%. В 68% случаев виновными оказываются сотрудники организаций, и только в 8% — руководство. По сравнению с 2015 годом количество утечек выросло на 89%. На сегодня Россия занимает второе после США место в списке стран, наиболее сильно страдающих от утечек информации. Причины возникновения угрозы информационной безопасности:

1. **Невнимательность и халатность сотрудников**. Угрозу информационной безопасности компании, как ни странно, могут представлять вполне лояльные сотрудники и не помышляющие о краже важных данных. Непредумышленный вред конфиденциальным сведениям причиняется по простой халатности или неосведомленности работников. Всегда есть возможность того, что кто-нибудь откроет фишинговое письмо и внедрит вирус с личного ноутбука на сервер компании. Или, например, скопирует файл с конфиденциальными сведениями на планшет, флэшку или КПК для работы в командировке. И ни одна компания не застрахована от пересылки невнимательным сотрудником важных файлов не по тому адресу. В такой ситуации информация оказывается весьма легкой добычей.

2. **Использование пиратского ПО**. Иногда руководители компаний пытаются сэкономить на покупке лицензионного ПО. Но следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного ПО не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Вместе с ним он покупает и вирусы, способные нанести вред системе компьютерной безопасности. По данным исследования Microsoft, в 7% изученных нелицензионных программ было найдено специальное программное обеспечение для кражи паролей и персональных данных.

3. **Вирусы.** Одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. В последние годы существенно увеличилась их частота и уровень ущерба. По мнению экспертов, это можно объяснить появлением новых каналов проникновения вирусов. На первом месте по-прежнему остается почта, но, как показывает практика, вирусы способны проникать и через программы обмена сообщениями, такие как ICQ и другие. Увеличилось и количество объектов для возможных вирусных атак. Если раньше атакам подвергались в основном серверы стандартных веб-служб, то сегодня вирусы способны воздействовать и на межсетевые экраны, коммутаторы, мобильные устройства, маршрутизаторы. В последнее время особенно активны стали так называемые вирусы-шифровальщики. Весной и летом этого года миллионы пользователей пострадали от атак вирусов WannaCry, Petya, Misha. Эпидемии показали, что жертвой вирусной атаки можно стать, даже если не открывать подозрительные письма. По информации Intel вирусом WannaCry заразились 530 тысяч компьютеров, а общий ущерб компаний составил более 1 млрд долларов.

4. **Угрозы со стороны совладельца бизнеса.** Именно легальные пользователи — одна из основных причин утечек информации в компаниях. Такие утечки специалисты называют инсайдерскими, а всех инсайдеров условно делят на несколько групп:

«Нарушители» — среднее звено и топ-менеджеры, позволяющие себе небольшие нарушения информационной безопасности — играют в компьютерные игры, делают онлайн-покупки с рабочих компьютеров, пользуются личной почтой. Такая безалаберность способна вызвать инциденты, но чаще всего они являются непредумышленными. Кстати, большинство внешних атак происходят именно через личные почтовые ящики или ICQ сотрудников.

«Преступники». Чаще всего инсайдерами являются топ-менеджеры, имеющие доступ к важной информации и злоупотребляющие своими привилегиями. Они самостоятельно устанавливают различные приложения, могут отсылать конфиденциальную информацию заинтересованным в ней третьим лицам и т.д.

«Кроты» — сотрудники, которые умышленно крадут важную информацию за материальное вознаграждение от компании-конкурента. Как правило, это весьма опытные пользователи, умело уничтожающие все следы своих преступлений. Поймать их в силу этого бывает очень непросто.

Еще одна категория — это уволенные и обиженные на компанию сотрудники, которые забирают с собой всю информацию, к которой они имели доступ. Обычно украденная информация используется ими на новом месте работы, целенаправленная продажа данных в России пока не слишком актуальна.

5. **Законодательные перипетии.** Государственные органы в России наделены правом конфисковать в ходе проверок оборудование и носители информации. Поскольку большая часть важных данных компании хранится в электронном виде на серверах, то в случае их изъятия компания на какое-то время просто останавливает свою деятельность. Простои при этом никто не компенсирует, а если проверка затягивается, большие убытки могут привести к прекращению деятельности фирмы. Изъятие оборудования — одна из острейших проблем современного бизнеса, при этом поводом для него может послужить все что угодно — от решения следователя до решения суда в рамках какого-либо уголовного дела.

# РАЗРАБОТКА СТРУКТУРЫ СЛУЖБЫ БЕЗОПАСНОСТИ С ОПИСАНИЕМ ОСНОВНЫХ ФУНКЦИЙ ПОДРАЗДЕЛЕНИЙ

Основными задачами службы безопасности предприятия являются:

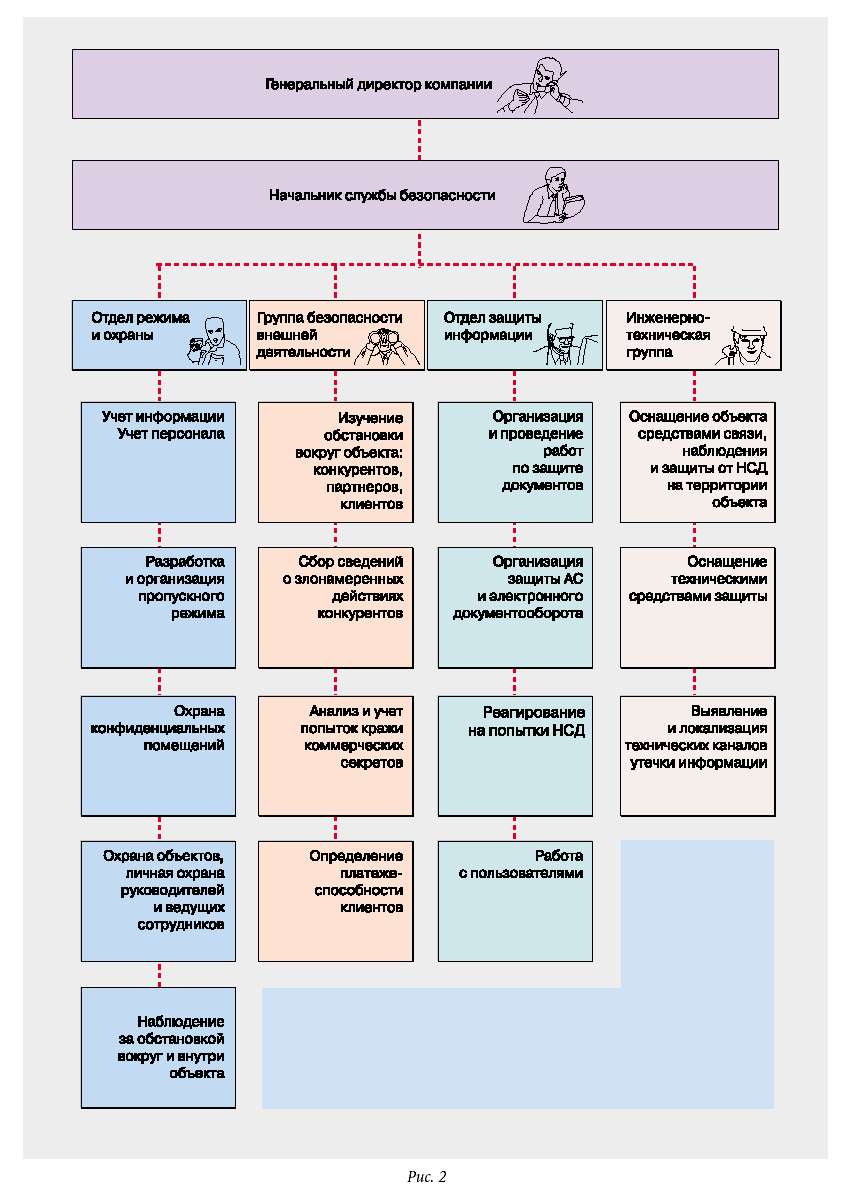
* обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
* организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
* организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
* предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
* выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
* обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;
* обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
* обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
* оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Служба безопасности предприятия выполняет следующие общие функции:

* организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
* руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
* участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
* разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны»;
* изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
* организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия; разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
* обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
* осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
* организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был осознанный подход;
* ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
* ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
* поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе.

Организационно служба безопасности состоит из следующих структурных единиц (рис. 2):

* отдел режима и охраны, в составе сектора режима и сектора охраны;
* отдел защиты информации;
* инженерно-техническая группа;
* группа безопасности внешней деятельности.



# ПЛАН ТЕРРИТОРИИ ПРЕДПРИЯТИЯ ИЛИ ПОЭТАЖНЫЕ ПЛАНЫ С ВЫДЕЛЕНИЕМ И ОБОЗНАЧЕНИЕМ ЗОН БЕЗОПАСНОСТИ, А ТАКЖЕ ПУТЕЙ ПРОХОДА В ЭТИ ЗОНЫ

Целью обеспечения физической безопасности предприятия является предотвращение неавторизированного физического доступа, повреждения и воздействия в отношении помещений и информации предприятия.

Границы пространства предприятия, защищаемого от угроз, называются рубежами защиты. Таких рубежей может быть несколько. Область пространства внутри замкнутого рубежа называется зоной безопасности.

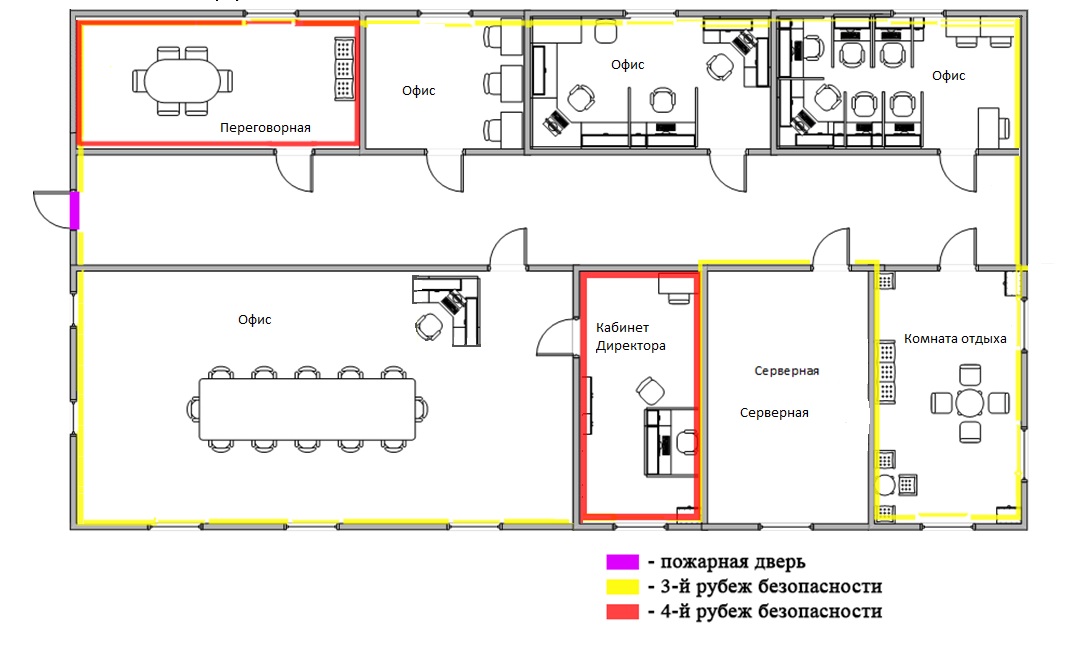
Можно выделить следующие рубежи защиты:

1-й рубеж. Периметр территории. Элементы ИТУ (забор, калитка, ворота).

2-й рубеж. Пространство между забором и строением. Элементы ИТУ, охранное освещение.

3-й рубеж. Периметр строения. Стены, окна, двери, СКУД и прочее.

4-й, 5-й, n-й рубежи. Зоны, которым необходима дополнительная защита (хранилища, кабинет руководителя и т.д.)



# РАЗРАБОТКА ДОЛЖНОСТНЫХ ИНСТРУКЦИЙ СОТРУДНИКОВ СЛУЖБЫ БЕЗОПАСНОСТИ

**Должностная инструкция директора службы безопасности**

УТВЕРЖДАЮ

Генеральный директор АО «Ласточка»

Быков И.П.

«\_\_\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ г.

**1. Общие положения**

1.1. Директор службы безопасности относится к категории руководителей.

1.2. Директор службы безопасности назначается на должность и освобождается от нее приказом генерального директора.

1.3. Директор службы безопасности подчиняется непосредственно генеральному директору.

1.4. На время отсутствия Директора службы безопасности его права и обязанности переходят к другому должностному лицу, о чем объявляется в приказе по организации.

1.5. На должность Директора службы безопасности назначается лицо, отвечающее следующим требованиям: высшее образование и стаж управленческой работы в соответствующей области не менее 3 лет.

1.6. Директор службы безопасности должен знать:

- законы и иные нормативно-правовые акты Российской Федерации, регламентирующие вопросы безопасности, частной охранной деятельности, защиты информации, оперативно-розыскной деятельности;

- принципы организации охраны объектов организации;

- технические средства защиты объектов от несанкционированного доступа к ним;

- технические средства защиты информации;

- требования к разработкам внутренних документов по режиму на объектах, инструкций по допуску к ресурсам предприятия (финансовым, товарно-материальным, информационным, пр.);

- правила сопровождения особо ценных товарно-материальных, финансовых и иных ресурсов;

- методы проведения инструктажа по безопасности, проведения контрольных мероприятий.

1.7. Директор службы безопасности руководствуется в своей деятельности:

- законодательными актами РФ;

- Уставом организации, Положением о службе безопасности, Правилами внутреннего трудового распорядка, другими нормативными актами компании;

- приказами и распоряжениями руководства;

- настоящей должностной инструкцией.

**2. Должностные обязанности Директора службы безопасности**

Директор службы безопасности выполняет следующие должностные обязанности:

2.1. Организует и возглавляет работу по правовой и организационной защите предприятия.

2.2. Разрабатывает и руководит мероприятиями по обеспечению безопасности охраняемых объектов.

2.3. Вырабатывает адекватные угрозе средства защиты и виды режимов охраны.

2.4. Осуществляет проверку и оценку лояльности сотрудником компании.

2.5. Обеспечивает неприкосновенность перевозимых материальных ценностей компании.

2.6. Обеспечивает соблюдение контрольно-пропускного режима.

2.7. Взаимодействует с правоохранительными органами в расследовании случаев преступных посягательств на охраняемые объекты.

2.8. Проводит обучение и тренинги персонала по вопросам безопасности.

2.9. Организует специальный режим делопроизводства, исключающий несанкционированное получение сведений, находящихся под режимом особого доступа.

2.10. Предотвращает необоснованный допуск и доступ к сведениям и работам, составляющим коммерческую тайну предприятия.

2.11. Оценивает необходимость привлечения для несения охраны объекта службы безопасности МВД, коммерческих охранных структур на договорной основе.

2.12. Контролирует соблюдение требований режима безопасности сотрудниками и посетителями.

2.13. Организует и проводит служебные расследования по фактам разглашения сведений, утрате документов, ценностей и других нарушений безопасности предприятия.

2.14. Возглавляет разработку основополагающих документов с целью закрепления в них требований по обеспечению безопасности предприятия (инструкции, положения, правила).

2.15. Вносит предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите безопасности предприятия.

2.16. Организует учет и анализ нарушений режима.

**3. Права Директора службы безопасности**

Директор службы безопасности имеет право:

3.1. Давать работникам обязательные для исполнения указания по безопасности предприятия.

3.2. Изучать личные дела работников предприятия.

3.3. Знакомиться с проектами решений руководства предприятия, касающимися деятельности службы безопасности.

3.4. Вносить на рассмотрение руководства предприятия предложения по улучшению деятельности службы безопасности.

3.5. Запрашивать от руководителей подразделений предприятия и специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей.

3.6. Подписывать и визировать документы в пределах своей компетенции.

3.7. Вносить на рассмотрение руководства предприятия представления о назначении, перемещении и увольнении сотрудников службы безопасности; предложения об их поощрении или о наложении на них взысканий.

3.8. Требовать от руководства компании оказания содействия в исполнении своих должностных обязанностей и прав.

**4. Ответственность Директора службы безопасности**

Директор службы безопасности несет ответственность:

4.1. За невыполнение и/или несвоевременное, халатное выполнение своих должностных обязанностей.

4.2. За несоблюдение действующих инструкций, приказов и распоряжений по сохранению коммерческой тайны и конфиденциальной информации.

4.3. За нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности.

РАЗРАБОТАЛ:

Директор по подбору персонала   
\_\_\_\_\_\_\_\_ Пупкин Д.О.

СОГЛАСОВАНО:   
Главный юрист

\_\_\_\_\_\_\_\_ Шуткин В.В.

Председатель профсоюзного комитета

\_\_\_\_\_\_\_\_ Берлинский В.Г.

ОЗНАКОМЛЕН:

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(подпись) (фамилия, инициалы)

**Должностная инструкция специалиста по информационной безопасности**

УТВЕРЖДАЮ

Генеральный директор АО «Ласточка»

Быков И.П.

«\_\_\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ г.

**1. Общие положения**

Специалист по информационной безопасности подчиняется непосредственно директору службы безопасности.

**2. Должностные обязанности специалиста по информационной безопасности**

Специалист по информационной безопасности выполняет следующие должностные обязанности:

2.1. Анализ и оценка потенциальных угроз безопасности.

2.2. Настройка брандмауэров и организация шифрования данных.

2.3. Мониторинг и проведение аудита систем.

2.4. В случае обнаружения отклонения от норм в работе систем, провести необходимые действия по устранению проблем.

2.5. Проведение тестовых атак на сеть предприятия, симулируя действия хакеров для поиска уязвимостей в программном обеспечении предприятия.

2.6. Проведение тестовых атак на сеть предприятия, используя сотрудников предприятия, симулируя действия социальных инженеров для проверки уровня усвоения персоналом инструкций по безопасности и для поиска неучтенных уязвимостей от атак, основанных на человеческом факторе.

2.7. Составление технических отчетов по результатам работы.

**3. Права специалиста по информационной безопасности**

Специалист по информационной безопасности имеет право:

3.1. Давать работникам предприятия обязательные для исполнения указания по безопасности предприятия.

3.2. Подписывать и визировать документы в пределах своей компетенции.

3.3. Изучать все стороны коммерческой, производственной, финансовой и другой деятельности предприятия для разработки и корректировки систем безопасности на предприятии.

3.4. Изучать личные дела работников предприятия.

3.5. Давать обязательные для выполнения указания персоналу и посетителям по соблюдению режима безопасности.

3.6. Давать рекомендации по соблюдению мер личной защиты ответственными работниками предприятия.

3.7. Знакомиться с документами, определяющими его права и обязанности по занимаемой должности, критерии оценки качества исполнения должностных обязанностей.

3.8. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.9. Требовать от руководства предприятия обеспечения организационно-технических условий и оформления установленных документов, необходимых для исполнения должностных обязанностей.

**4. Ответственность специалиста по информационной безопасности**

Специалист по информационной безопасности несет ответственность:

4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, — в пределах, установленных действующим трудовым законодательством Российской Федерации.

4.2. За правонарушения, совершенные в процессе своей деятельности, — в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.3. За причинение материального ущерба предприятию — в пределах, установленных действующим трудовым и гражданским законодательством Российской Федерации.

РАЗРАБОТАЛ:

Директор службы безопасности   
\_\_\_\_\_\_\_\_ Иванов Е.Н.

СОГЛАСОВАНО:   
Главный юрист

\_\_\_\_\_\_\_\_ Петров В.В.

Директор по подбору персонала

\_\_\_\_\_\_\_\_ Воропаев Д.О.

Председатель профсоюзного комитета

\_\_\_\_\_\_\_\_ Сидоров В.Г.

ОЗНАКОМЛЕН:

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(подпись) (фамилия, инициалы)

**Должностная инструкция коммерческого директора**

УТВЕРЖДАЮ

Генеральный директор АО «Ласточка»

Быков И.П.

«\_\_\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ г.

**1. Общие положения**

1.1. Коммерческий директор относится к категории руководителей.

1.2. Коммерческий директор назначается на должность и освобождается от нее приказом генерального директора.

1.3. Коммерческий директор подчиняется непосредственно генеральному директору.

1.4. На время отсутствия коммерческого директора его права и обязанности переходят к другому должностному лицу, о чем объявляется в приказе по организации.

1.5. На должность коммерческого директора назначается лицо, отвечающее следующим требованиям: высшее профессиональное образование и стаж управленческой работы в соответствующей области не менее 3 лет.

1.6. Коммерческий директор должен знать:

- коммерческое, гражданское, финансовое законодательство;

- профиль, специализацию, особенности структуры предприятия;

- перспективы технического и финансово-экономического развития предприятия;

- порядок разработки бизнес-планов;

- основные принципы финансового планирования;

- порядок заключения и оформления хозяйственных и финансовых договоров.

1.7. Коммерческий директор руководствуется в своей деятельности:

- законодательными актами РФ;

- Уставом организации, Правилами внутреннего трудового распорядка, другими нормативными актами компании;

- приказами и распоряжениями руководства;

- настоящей должностной инструкцией.

**2. Должностные обязанности коммерческого директора**

Коммерческий директор выполняет следующие должностные обязанности:

2.1. Организует руководство материально-техническим снабжением предприятия, деятельностью по хранению, транспортировке и сбыту продукции (продаже товаров, оказанию услуг).

2.2. Координирует разработку и составление перспективных и текущих планов материально-технического обеспечения и сбыта продукции (продажи товаров, оказания услуг), финансовых планов.

2.3. Координирует разработку нормативов и стандартов материально-технического обеспечения (запасов материально-технических ресурсов), стандартов качества продукции (товаров, услуг), хранения готовой продукции (товаров), нормативов запасов готовой продукции (товаров).

2.4. Дает рекомендации и консультации менеджерам и специалистам по финансовому планированию, сбыту, продаже; контролирует их работу.

2.5. Обеспечивает своевременное составление сметно-финансовых и других документов, расчетов, отчетов о выполнении планов материально-технического снабжения, по сбыту готовой продукции (продаже товаров), финансовой деятельности.

2.6. Осуществляет контроль за финансовыми и экономическими показателями деятельности предприятия, расходованием финансовых средств.

2.7. Проводит переговоры от имени предприятия с контрагентами предприятия по хозяйственным и финансовым сделкам, заключает от имени предприятия хозяйственные и финансовые договоры, обеспечивает выполнение договорных обязательств.

2.8. Участвует от имени предприятия в ярмарках, торгах, на биржах, выставках по рекламе и реализации продукции (товаров, услуг).

**3. Права коммерческого директора**

Коммерческий директор имеет право:

3.1. Представлять интересы предприятия во взаимоотношениях с государственными органами, сторонними организациями и учреждениями по коммерческим вопросам.

3.2. Устанавливать служебные обязанности для подчиненных работников.

3.3. Запрашивать от структурных подразделений предприятия информацию и документы, необходимые для выполнения его должностных обязанностей.

3.4. Участвовать в подготовке проектов приказов, инструкций, указаний, а также смет, договоров и других документов, связанных с решением коммерческих вопросов.

3.5. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.6. Требовать от руководства предприятия обеспечения организационно-технических условий и оформления установленных документов, необходимых для исполнения должностных обязанностей.

**4. Ответственность коммерческого директора**

Коммерческий директор несет ответственность:

4.1. За невыполнение и/или несвоевременное, халатное выполнение своих должностных обязанностей.

4.2. За несоблюдение действующих инструкций, приказов и распоряжений по сохранению коммерческой тайны и конфиденциальной информации.

4.3. За нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности.

РАЗРАБОТАЛ:

Директор по подбору персонала  
\_\_\_\_\_\_\_\_ Иванов Д.О.

СОГЛАСОВАНО:   
Главный юрист

\_\_\_\_\_\_\_\_ Петров В.В.

Председатель профсоюзного комитета

\_\_\_\_\_\_\_\_ Берлинский В.Г.

ОЗНАКОМЛЕН:

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(подпись) (фамилия, инициалы)

# РАЗРАБОТКА ДОКУМЕНТА «ПОЛИТИКА ИБ ОРГАНИЗАЦИИ»

**Политика безопасности**

1. **Введение**

Для достижения поставленной цели Компании предстоит решить широкий комплекс задач, направленных на повышение эффективности и стабильности функционирования бизнеса.

Учитывая тенденции развития мировой и отечественной экономики, в соответствии с которыми, информация и информационные технологии становятся важнейшими активами современного бизнеса, способствующими повышению его конкурентоспособности, Компания уделяет особое внимание решению задачи обеспечения информационной безопасности.

Под информационной безопасностью Компания понимает состояние защищенности своих интересов (целей) от угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационных активов: конфиденциальности, целостности и доступности.

Обеспечение информационной безопасности Компании осуществляется в рамках циклической модели менеджмента информационной безопасности: «планирование — реализация — проверка — совершенствование», отвечающей принципам и модели корпоративного менеджмента в Компании.

Политика информационной безопасности (далее – Политика) устанавливает цели, задачи и принципы в области информационной безопасности, которыми руководствуется Компания в своей деятельности.

Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

1. **Область применения**

Положения Политики распространяются на всех работников Компании, имеющих доступ к информационным активам и ИТ-инфраструктуре Компании, а так же учитываются в отношениях с контрагентами (потребителями продукции, поставщиками, партнерами, консультантами, стажерами, практикантами и т.д.).

1. **Цели Компании в области информационной безопасности**

Важнейшими целями Компании в области информационной безопасности являются:

* Повышение конкурентоспособности бизнеса Компании;
* Соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;
* Повышение деловой репутации и корпоративной культуры Компании;
* Достижение адекватности мер по защите от угроз информационной  безопасности;
* Предотвращение и (или) снижение ущерба от реализации угроз информационной безопасности.

1. **Принципы реализации политики**

При достижении поставленных целей Компания намерена руководствоваться следующими принципами:

а) **Вовлеченность высшего руководства Компании в процесс обеспечения информационной безопасности.** Деятельность по обеспечению информационной безопасности инициирована и контролируется высшим руководством Компании. Координация деятельности по обеспечению информационной безопасности осуществляется в рамках действующего в Компании комитета, в состав которого входят представители высшего руководство. Высшее руководство Компании выполняет те же правила по обеспечению информационной безопасности, что и все работники Компании.

б) **Законность обеспечения информационной безопасности.** Компания реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами.

в) **Согласованность действий по обеспечению информационной, физической и экономической безопасности.** Действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений Компании и согласованы между собой по целям, задачам, принципам, методам и средствам.

г) **Экономическая целесообразность.** Компания стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.

д) **Знание своих работников.** Компания стремится тщательно подбирать персонал (работников), вырабатывать и поддерживать корпоративную этику, что создает благоприятную среду для деятельности Компании и снижает риски информационной безопасности.

е) **Документированность требований информационной безопасности.** Компания стремится, чтобы все требования в области информационной безопасности были зафиксированы во внутренних нормативных документах, утвержденных руководством Компании.

ж) **Осведомленность в вопросах обеспечения информационной безопасности.** Документированные требования в области информационной безопасности доводятся до сведения работников Компании и контрагентов в части их касающейся. Компания на периодической основе осуществляет информирование, обучение и аттестацию работников по вопросам обеспечения информационной безопасности.

з) **Реагирование на инциденты информационной безопасности.** Компания стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности.

и) **Персональная ответственность.** Работники Компании несут персональную ответственность за соблюдение требований информационной безопасности. Обязанности по обеспечению информационной безопасности включаются в трудовые договоры и должностные инструкции работников, а так же в договоры (соглашения) с контрагентами.

к) **Учет действий с информационными активами.** Компания стремится вести учет всех действий работников Компании и контрагентов с информационными активами Компании.

л) **Предоставление минимально необходимых прав доступа.** Работникам Компании и контрагентов предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств. При этом Компания стремится предоставлять права доступа таким образом, чтобы выполнение особо важной (критичной) операции осуществлялось с участием как минимум двух работников.

м) **Учет требований информационной безопасности в проектной деятельности.** Помимо операционной деятельности, Компания стремится учитывать требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.

1. **Заинтересованные стороны**

Заинтересованными сторонами при реализации Политики Компания считает:

* акционеров и потенциальных инвесторов;
* органы государственной власти;
* контрагентов (потребители продукции, поставщики и т.д.) и деловых партнеров (потенциальные контрагенты, дочерние и зависимые общества и т.д.);
* работников.

Организация эффективного взаимодействия Компании с заинтересованными сторонами способствует повышению капитализации Компании, долгосрочному постоянному развитию и непрерывности бизнеса, снижению рисков инвестиций, соблюдению требований законодательства и договорных обязательств в части информационной безопасности, обеспечению высокой деловой репутации Компании, обеспечению своевременной поставки продукции, повышению квалификации работников и корпоративной культуры.

Компания обеспечивает защиту конфиденциальной информации, полученной от заинтересованной стороны на уровне, разумно достаточном для заинтересованной стороны, но не меньшем, чем уровень защиты собственной конфиденциальной информации.

1. **Документационное обеспечение**

Компания разрабатывает и внедряет внутренние нормативные документы по обеспечению информационной безопасности на основе законодательных требований, а так же положений международных и национальных стандартов в области информационной безопасности:

* долгосрочную программу мероприятий по обеспечению информационной безопасности;
* стандарты, положения и инструкции по обеспечению информационной безопасности;
* планы обеспечения непрерывности бизнеса и действий в случаях чрезвычайных ситуаций.

Кроме того, Компания на периодической основе проводит анализ внутренних нормативных документов на предмет их эффективности и непротиворечивости, а так же поддерживает данные документы в актуальном состоянии.

Политика пересматривается не реже одного раза в два года.

1. **Управление рисками**

Активная позиция руководства Компании в вопросах управления рисками информационной безопасности выражается в поддержке регулярной деятельности по следующим направлениям:

* Идентификация и классификация активов, подлежащих защите, и определение владельцев этих активов.
* Своевременное выявление и прогнозирование угроз информационной безопасности в отношении идентифицированных активов.
* Оценка вероятности реализации угроз информационной безопасности и степени их влияния на бизнес Компании на основе методов, позволяющих обеспечить сравнимые и воспроизводимые результаты.
* Обработка рисков информационной безопасности.
* Оценка эффективности применяемых методов и средств обеспечения информационной безопасности, в том числе с привлечением внутренних и внешних аудиторов.

1. **Стратегические инициативы**

Для достижения поставленных целей в области обеспечения информационной безопасности Компания намерена осуществлять:

* Внедрение системы менеджмента информационной безопасности в соответствии с международным стандартом ISO/IEC 27001:2005 «Information Technology. Security techniques. Information security management systems. Requirements».
* Сертификацию особо важных (критичных) для деятельности Компании бизнес-процессов на соответствие международному стандарту ISO/IEC 27001:2005 «Information Technology. Security techniques. Information security management systems. Requirements».
* Внедрение передовых программных, аппаратных и технических решений в области информационной безопасности.

# ЗАКЛЮЧЕНИЕ

В процессе выполнения работы была составлена структура вымышленного предприятия АО «Ласточка», включая все подразделения компании, в том числе, службу безопасности. Были выделены основные информационные потоки внутри предприятия, с учетом которых был проведен анализ возможных путей утечки конфиденциальной информации и угроз информационной безопасности.

Одна из главных задач состояла в организации автоматизированной системы защиты. Для ее выполнения была выбрана система контроля и управления доступом, и был проведен ее анализ на техническом и прикладном уровне. Кроме того, была составлена схема предприятия с выделением зон безопасности, разработаны должностные инструкции сотрудников службы безопасности и политика безопасности защищаемого предприятия.

Таким образом, была достигнута основная цель настоящей курсовой работы, заключающаяся в организации информационной защиты предприятия.

# СПИСОК ЛИТЕРАТУРЫ

1. Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. - СПб: Университет ИТМО, 2013.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149 ФЗ.

3. Герасименко В. А., Мецатунян М.В. Организация комплексной защиты информации на современных объектах//Вопросы защиты информации, № 1, 1995.

4. Иванов И. Г., Кузнецов П. А., В. И., Попов В. И. Методические основы защиты информации в банковских автоматизированных комплексах//Защита информации. Конфидент, № 1, 1994.

5. ГОСТ Р 56546-2015. Классификация уязвимостей информационных систем. – Введ. 19.08.2015.– М: Стандартинформ.

6. Методика определения угроз безопасности информации в информационных системах: ФСТЭК России // Методический документ. – 2015 – 43 с.

7. Статья «Модель нарушителя в системе безопасности» [Электронный ресурс] / Secuteck.-:URL: http://www.secuteck.ru/articles2/OPS/model-narushitela.