**ВВЕДЕНИЕ**

Компьютеризация, начавшаяся в 20 веке, длится по сей день. Информационные системы (ИС) повышают производительность труда любой организации. Пользователи могут быстро получать данные необходимые для выполнения их обязанностей. Однако у компьютеризации есть другая сторона: злоумышленники получают облегчение доступа к базам данных. Обладая доступом к различным базам данных (БД), злоумышленники могут использовать их для вымогания денег, других ценных сведений, материальных ценностей и прочего.

Поэтому в наше время защита информации стоит на первом месте. Чаще всего злоумышленников интересуют сведения, хранящиеся в БД государственных структур, таких как МВД, Центробанк и т.д., а также подконтрольных им организациям, таким как учреждения здравоохранения, образования. Всё чаще в СМИ появляются статьи, на тему популярных SMS-мошенничеств. А ведь получив доступ к БД какой-нибудь финансовой организации, злоумышленник может бесконтрольно делать денежные переводы, либо получить доступ к конфиденциальным сведениям, и продавать информацию о клиентах.

Защита персональных данных является актуальной темой в нашей стране, поскольку законодательная база существует менее 10 лет. В связи с тем, часто лица, ответственные за обработку персональных данных не знаю элементарных правил безопасности доверенной им информации. Поэтому на специалистов по информационной безопасности ложиться не только ответственность за безопасность информационной системы, но и система обучения персонала.

Данная работа посвящена разработке программной системы безопасности кондитерской фирмы.

**1. Программные средства безопасности**

* 1. **Назначение программного обеспечения систем безопасности**

Средства защиты объединяют отдельные устройства в охранный комплекс, поддерживают пропускной режим, фиксируют события, дают возможность вносить изменения, удаленно контролировать ситуацию, оперативно управлять техникой, разрабатывать и встраивать новые алгоритмы. ПО управляет оборудованием централизованно и на каждом рабочем месте, со строгой иерархией, разделением уровней.

Основные задачи, которые помогает выполнять ПО:

Дистанционный контроль, наблюдение за территорией по изображениям с камер видеонаблюдения, показаниям датчиков, извещателей, разграничение доступа сотрудников, высокая степень программной части защиты. Автоматика визуализирует информацию: показывает схемы, ситуационные планы, транслирует видеосигнал с камер в точках срабатывания. Удаленное управление, настройка. Оператор центрального пульта может переключать режимы, регулировать оборудование, контролировать состояние защитной техники. Разделение прав доступа. В программу вносят сведения о каждом сотруднике. При необходимости объект разделяют на зоны с разными уровнями, корректируют алгоритм работы СКУД, создают локальные и централизованные пункты управления, используют сложные и нестандартные алгоритмы доступа. Ведение протоколов. Автоматика записывает события, сохраняет видеозаписи при срабатывании извещателей, фиксирует время прохода, хранит картотеку пропусков, идентификационные сведения и другую информацию. Долгосрочное хранение помогает формировать ретроспективные отчеты. ПО делает работу охранного комплекса взаимосвязанной и эффективной, оборудование проще настраивать, эксплуатировать, контролировать, проводить диагностику, модернизацию, ремонт. Программа интегрируется в существующую сеть, объединяет разнотипные подсистемы.

На кондитерских фабриках обычно используются различные программные средства защиты, обеспечивающие безопасность производства и сохранность продукции. Некоторые из распространенных программных средств защиты включают:

* Антивирусное программное обеспечение: для защиты компьютерных систем и сетей от вирусов, таких как вирусы, трояны и шпионское ПО.
* Брандмауэры.
* Системы мониторинга и обнаружения вторжений (IDS/IPS):
* Системы резервного копирования данных.
* Системы управления доступом: позволяют контролировать физический доступ к зоне производства, складам и важным областям, используя механические или электронные средства идентификации.
* Управление и мониторинг систем: Программное обеспечение, которое занимает централизованное управление и мониторинг компьютерных систем, сетей и безопасности.
* Шифрование данных: используется для защиты конфиденциальности информации о передаче ее в неразборчивую форму для неавторизованных пользователей.

Это всего лишь несколько примеров программных средств защиты, которые применяются на кондитерских фабриках. Конкретные средства защиты будут зависеть от конкретных требований и безопасности каждой фабрики.

**1.2 Классификация угроз**

Под угрозой (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам.

Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз информационной безопасности обусловлена тем, что хранимая и обрабатываемая информация в современных АС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Классификация возможных угроз информационной безопасности может быть проведена по следующим базовым признакам:

По природе возникновения:

естественные угрозы, вызванные воздействиями объективных физических процессов или стихийных природных явлений;

искусственные угрозы безопасности, вызванные деятельностью человека.

По степени преднамеренности проявления:

угрозы, вызванные ошибками или халатностью персонала, например некомпетентное использование средств защиты, ввод ошибочных данных и т.п.;

угрозы преднамеренного действия, например действия злоумышленников.

По непосредственному источнику угроз:

природная среда, например стихийные бедствия, магнитные бури и пр.;

человек, например: вербовка путем подкупа персонала, разглашение конфиденциальных данных и т.п.;

санкционированные программно-аппаратные средства, например удаление данных, отказ в работе ОС;

несанкционированные программно-аппаратные средства, например заражение компьютера вирусами с деструктивными функциями.

По положению источника угроз:

вне контролируемой зоны, например перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств;

в пределах контролируемой зоны, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.;

непосредственно внутри, например некорректное использование ресурсов АС.

По степени зависимости от активности:

независимо от активности АС, например вскрытие шифров криптозащиты информации;

только в процессе обработки данных, например угрозы выполнения и распространения программных вирусов.

По степени воздействия на АС:

пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС, например угроза копирования секретных данных;

активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС, например внедрение троянских коней и вирусов.

По этапам доступа пользователей или программ к ресурсам:

угрозы, проявляющиеся на этапе доступа к ресурсам АС, например: угрозы несанкционированного доступа в АС;

угрозы, проявляющиеся после разрешения доступа к ресурсам АС, например угрозы несанкционированного или некорректного использования ресурсов АС.

По способу доступа к ресурсам:

Угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам АС.

Угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам АС, например: несанкционированный доступ к ресурсам АС путем использования недокументированных возможностей ОС.

По текущему месту расположения информации, хранимой и обрабатываемой в АС:

Угрозы доступа к информации, находящейся на внешних запоминающих устройствах, например: несанкционированное копирование секретной информации с жесткого диска;

Угрозы доступа к информации, находящейся в оперативной памяти, например: чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ;

Угрозы доступа к информации, циркулирующей в линиях связи, например: незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;

Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере, например: запись отображаемой информации на скрытую видеокамеру.

Опасные воздействия на АС подразделяются на случайные и преднамеренные.

Причинами случайных воздействий при эксплуатации АС могут быть:

аварийные ситуации из-за стихийных бедствий и отключений электропитания;

* отказы и сбои аппаратуры;
* ошибки в программном обеспечении;
* ошибки в работе обслуживающего персонала и пользователей;
* помехи в линиях связи из-за воздействий внешней среды.

Ошибки в программном обеспечении (ПО) являются распространенным видом компьютерных нарушений. ПО серверов, рабочих станций, маршрутизаторов и т.д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (использование компьютера в качестве плацдарма для атаки и т.п.). Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя может быть служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т.п.

* 1. **Регуляция**

Национальное российское законодательство в этой сфере проработано неравномерно, наиболее полно отрегулированы три блока:

* Государственная тайна;
* персональные данные;
* коммерческая тайна.

Вопрос раскрывается в нескольких федеральных законах и подзаконных актах, часто содержащих пересекающиеся нормы. Правоприменение обычно реализуется в рамках трудовых договоров и внутренних нормативных актов компаний.

149-ФЗ - Федеральный закон «Об информации» не внес в российское правовое поле каких-либо существенных норм в части регулирования оборота данных, но утвердил, какая именно информация окажется закрытой, опираясь на критерий ограниченности доступа к ней.

Исходя из ст. 9 закона, к этой категории относятся:

* государственная тайна;
* служебная информация госструктур;
* коммерческая тайна;
* служебная тайна;
* персональные данные;
* профессиональная тайна.

Закон не устанавливает никаких особых требований к обеспечению безопасности закрытой в доступе информации, адресуя к федеральным законам, регулирующим конкретные сферы правоотношений. Дополнительно он определяет критерий общедоступности информации, исключающий ее отнесение к категории данных ограниченного доступа. Также он раскрывает вопросы государственного регулирования информационных систем, обрабатывающих данные высокой степени секретности.

Закон о коммерческой тайне, ГК РФ и ТК РФ:

Применительно к коммерческой тайне компаний, в России работают три нормативных акта – федеральный закон «О коммерческой тайне», Гражданский кодекс и Трудовой кодекс.

ФЗ «О коммерческой тайне» рассматривает: способы отнесения данных к коммерческой тайне и механизмы ее защиты. Закон полностью отдает этот вопрос на откуп компаниям, не выделяя критериев, которые могли бы доказать действительную ценность информации, за разглашение которой гражданину может грозить уголовная ответственность;

Перечень сведений, которые не могут быть отнесены к коммерческой тайне. По сути он ограничен общедоступной информацией;

Способы охраны данных, в общем идентичные списку организационных мер, рекомендованных для защиты персональных данных.

Компания вправе назвать коммерческой тайной практически любые данные, за их разглашение сотрудник понесет ответственность в рамках гражданского и уголовного законодательства. Гражданский кодекс ранее содержал ст. 139, посвященную вопросам коммерческой тайны и способам привлечения граждан к имущественной ответственности за ее разглашение, недавно она была исключена. Сейчас работодатель может привлечь сотрудника к ответственности только в рамках ст. 15, говорящей о возмещении убытков.

Законодатель принял сторону работника, утвердив, что убытки могут быть возмещены только после того, как будут установлены:

* их фактическое существование;
* их реальная оценка.

В большинстве случаев сделать это невозможно, так как доказать реальную стоимость утраченных сведений, если в список сведений, относимых к коммерческой тайне, включено все, что пришло в голову администрации, фактически невозможно. Тем не менее в рамках трудового права работника можно уволить за утечку закрытых данных любого характера и любой ценности.

Включить условие о неразглашении охраняемой законом тайны в стандартный трудовой договор позволяет ст. 57 ТК РФ.

**1.4 Контроль доступа и системы обнаружения вторжений**

Контроль доступа к данным – это метод обеспечения безопасности, с помощью которого можно регулировать процесс предоставления прав на использование ресурсов информационной среды. Это фундаментальная концепция безопасности, которая работает на снижение рисков информационной безопасности. Обязательными компонентами контроля доступа в организации должны быть соответствующая методология, разработанные процедуры, а также технические средства, которые обеспечивают контроль. В наше время уже практически во всех компаниях первые два из трех компонентов присутствуют. Также многие организации идут по пути повышения зрелости процессов ИБ и постепенно внедряют автоматизированные инструменты, позволяющие повысить эффективность и безопасность бизнес-процессов.

Контроль доступа может быть физическим и логическим (техническим). Физический контроль ограничивает доступ к помещениям: зданиям, объектам внутри зданий или к физическим активам. Логический контроль ограничивает подключение к сетям, файлам, данным, хранящимся на информационных ресурсах.

Чтобы защитить информацию и сделать доступ безопасным, используются специализированные системы (IdM/IGA), которые позволяют управлять учетными данными пользователей и обеспечивают предоставление и разграничение прав доступа к информационным ресурсам компании для этих учетных данных. В некоторых случаях такие системы интегрируются с решениями, ограничивающими доступ к зданиям и физическим объектам (СКУД), или со специализированными решениями, которые в режиме реального времени предотвращают попытки несанкционированного доступа, например с PAM-системами, или с другими смежными решениями, – тем самым повышая защиту информационных активов предприятия.

IGA принято считать эволюцией систем класса IdM (Identity Management). На Западе уже практически ушли от использования аббревиатуры IdM. В России и СНГ эти понятия пока отождествляются, и их часто используют вместе, например, так: IdM/IGA-система Solar inRights.

Оба решения выполняют схожие функции. Но есть некоторые различия в подходах. В IdM в центре внимания – целевые системы и учетные записи в них. В IGA – пользователь. Такой подход позволяет реализовать ролевую модель управления доступом, обуславливает лучшую гибкость решений и большие возможности по администрированию/управлению правами и полномочиями. И он используется все чаще.

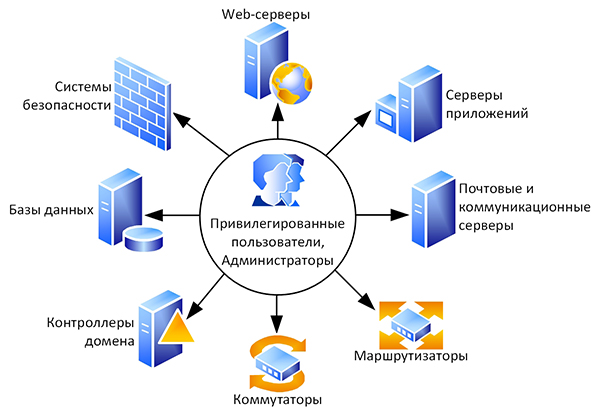


Рисунок 1. Контроль привилегированных пользователей

Контроль привилегированных пользователей, или Privileged Account Management (PAM) – это группа решений, предназначенных для осуществления мониторинга и контроля учетных записей сотрудников IT-подразделений, системных администраторов, сотрудников аутсорсинговых организаций, занимающихся администрированием инфраструктуры компании, управления аутентификацией и авторизацией указанных сотрудников, аудита выполняемых действий, контроля доступа и записи их сессий. Помимо аббревиатуры PAM для обозначения систем контроля привилегированных пользователей, встречаются другие наименования данного класса решений, например, Privileged User Management (PUM), Privileged Identity Management (PIM), Privileged Access Management (PAM), Privileged Password Management (PPM), Privileged Account Security (PAS). Решения, позволяющие контролировать действия учетных записей сотрудников, имеющих расширенные права, относятся к группе систем управления учетными данными (IdM/IAM-системы). Требования по мониторингу действий, выполняемых от имени учетных записей с повышенными привилегиями, возникли в связи с потребностью многих организаций передавать некоторые задачи администрирования и обслуживания инфраструктуры в руки сторонних организаций. Передача критичных ресурсов на IT-аутсорсинг подразумевает под собой серьезные риски. PAM-системы подразумевают под собой наличие следующих функций: Централизованное управление учетными записями с расширенными возможностями; Аудит действий привилегированных сотрудников; Управление настройками парольной защиты; Контроль доступа сотрудников к административным ресурсам; Управление процессом аутентификации и авторизации; Запись сессии, запущенной из-под учетной записи из списка привилегированных.

Системы IDS и IPS:

IDS (система наблюдения и обнаружения вторжений) и IPS (система предотвращения вторжений) — это программные средства защиты, которые широко применяются для обнаружения и предотвращения несанкционированного доступа и атак на компьютерные системы и сети.

IDS (система наблюдения и выявления вторжений) — это инструмент, который контролирует активность сети и выявляет признаки, указывающие на возможные последствия вторжений или аномальное поведение в сети. Он анализирует сетевой трафик, пакеты данных, системные журналы и другие источники информации, чтобы обнаруживать атаки или необычайную активность. IDS может использовать различные методы обнаружения, такие как сигнатурное обнаружение (сопоставление с ранее выявленными шаблонами зловредного кода), аномальное обнаружение (выявление необычных или аномальных паттернов активности).

IPS (система предотвращения вторжений) работает на основе функциональности IDS, но имеет дополнительную возможность предотвращения взлома в режиме реального времени. В отличие от IDS, которая только обнаруживает и предупреждает об атаках, IPS принимает активные меры для предотвращения несанкционированного доступа или атак. Он может автоматически блокировать трафик, который соответствует заданным правилам или сигнатурам, отбрасывать подозрительные пакеты данных или принимать меры по предупреждению, чтобы снизить риск взлома.

Системы IDS/IPS могут быть реализованы в виде аппаратных или программных устройств, которые отслеживают трафик в пределах сети или через сетевые узлы.

Система контроля и управления доступом:

СКУД (система контроля и управления доступом) — это программно-аппаратный комплекс, предназначенный для контроля доступа людей к определенным помещениям, зонам или ресурсам. СКУД обеспечивает автоматизированное управление и мониторинг доступа, а также регистрацию событий, связанных с прохождением людей через контрольные точки.

Принцип работы СКУД включает в себя несколько ключевых компонентов:

Контроллеры доступа: это аппаратные устройства, установленные на точках входа (двери, турникеты и т.д.). Они обеспечивают физический контроль доступа и взаимодействуют с программным обеспечением СКУД. Контроллеры могут быть оснащены считывателями карт, биометрическими устройствами (например, сканерами отпечатков пальцев) или другими средствами идентификации.

Средства идентификации: СКУД — это программно-аппаратный комплекс, который используется для ограничения и контроля физического доступа людей к определенным помещениям, зонам или ресурсам внутри организации или объекта.

Основной целью СКУД является обеспечение безопасности и контроля доступа путем идентификации пользователей, управления правами доступа и регистрации событий, связанных с физическим доступом. Вот некоторые основные компоненты и функциональные возможности СКУД:

Идентификация пользователей: СКУД позволяет идентифицировать пользователей, используя различные методы, такие как проходные карточки, брелоки, биометрические данные (отпечатки пальцев, сетчатка глаза и т. д.), ПИН-коды или комбинации этих методов. Каждый пользователь имеет уникальные учетные данные, которые используются для проверки их подлинности при попытке доступа.

Контроль доступа: СКУД позволяет настроить права доступа для каждого пользователя или группы пользователей. Администраторы могут определить, к каким зонам или помещениям имеет доступ каждый пользователь, и задать ограничения на время доступа (например, доступ только в определенные часы). Это позволяет эффективно управлять доступом и предотвращать несанкционированный доступ.

Управление событиями: СКУД регистрирует и сохраняет информацию о всех событиях, связанных с доступом, таких как успешные и неуспешные попытки доступа, время входа и выхода, двери, которые были открыты или закрыты, и т. д. Это позволяет проводить аудит и анализ доступа, а также расследовать инциденты безопасности.

Интеграция с другими системами безопасности: СКУД может быть интегрирована с другими системами безопасности, такими как системы видеонаблюдения, пожарной сигнализации или системы управления зданием. Это позволяет создать согласованную и централизованную систему безопасности, которая обеспечивает более эффективное реагирование на инциденты.

Удаленное управление: СКУД может предоставлять возможность удаленного управления и мониторинга. Администраторы могут контролировать доступ и получать уведомления о событиях через веб-интерфейс или мобильное приложение.

Гибкость и масштабируемость: СКУД может быть настроена и масштабирована под нужды организации. Она может включать различные типы считывателей, электромагнитные замки, кнопки выхода, сигнальные устройства и другое оборудование, а также поддерживать большое количество пользователей и точек доступа.

Важно отметить, что СКУД является одной из мер безопасности и должна использоваться в сочетании с другими мерами, такими как физические барьеры, видеонаблюдение, обучение персонала и политики безопасности, для обеспечения комплексной системы защиты.

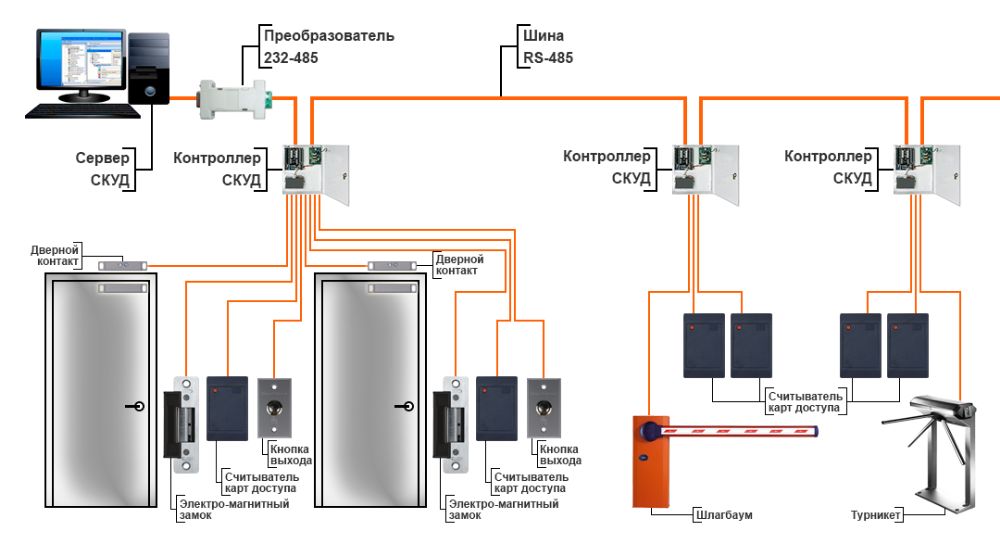


Рисунок 2. Схема монтажа скуд

**2. Проектирование программной системы безопасности на предприятии**

**2.1 технико-экономическая характеристика предприятия**

Полное наименование организацииОАО «РОТ ФРОНТ» в составе Холдинга «Объединенные кондитеры» входит в Холдинговую компанию «ГУТА».

Фабрика «РОТ ФРОНТ» стала первым кондитерским предприятием, которое в 2001 году вошло в Группу «ГУТА». Это был первый шаг, с которого началось становление Холдинга «Объединенные кондитеры».

Сегодня Группа «ГУТА» объединяет компании, деятельность которых затрагивает не только пищевую промышленность, но и строительство, недвижимость, страхование, медицину, а также индустрию красоты и здоровья.

Группа «Гута» привлекает инвестиции и реализует крупномасштабные проекты в наиболее динамично развивающихся отраслях экономики, сотрудничает с деловыми, правительственными и общественными организациями, чтобы достигнуть максимальных результатов, активно выступает в защиту интеллектуальной собственности, вкладывает средства в развитие медицины, физической культуры и спорта, воспитание молодежи.

Компания стремится в полной мере соответствовать международным требованиям в области охраны окружающей среды и стандартов качества.

Открытое Акционерное Общество "РОТ ФРОНТ" является одним из старейших производителей кондитерских изделий в России.

Организационная структура предприятия – это форма разделения труда, закрепляющая определенные функции управления за структурными подразделениями различного уровня иерархии.

Организационная структура управления предприятием адекватна структуре самого предприятия и соответствует масштабам и функциональному назначению управляемых объектов. Крупные предприятия, специализирующиеся на производстве сложных и трудоемких видов продукции (например, автомобилей, самолетов, металлов, нефтепродуктом и др.) состоят, как правило, из десятков цехов, лабораторий и отделов. Для координации их деятельности создается сложная иерархическая структура управления.

|  |  |
| --- | --- |
| Факторы, определяющие сложность организационной структуры предприятия | Как влияет усиление (увеличение, повышение, углубление) фактора |
| Номенклатура выпускаемой продукции | осложняет |
| Показатель унификации продукции | упрощает |
| Сложность продукции | осложняет |
| Масштаб производства | упрощает |
| Специализация производства | упрощает |
| Кооперирование производства | упрощает |
| Концентрация производства | осложняет |
| Комбинирование производства | осложняет |

Рисунок 3. Принципы организации предприятия и структуры аппарата управления

1. Управление предприятием осуществляется в соответствии с Уставом предприятия, настоящим Положением.

2. Организационная структура предприятия включает в себя наименование структурных подразделений предприятия, их основные функции и административную, функциональную подчиненность.

3. Общее управление предприятием осуществляет генеральный директор предприятия.

Статус, порядок назначения и освобождения от должности генерального директора определяется законодательством РФ и Уставом предприятия. В случае отсутствия на предприятии генерального директора его функции осуществляет заместитель, назначенный приказом генерального директора.

4. Руководство структурными подразделениями осуществляют главный инженер и заместители генерального директора предприятия, которые назначаются и освобождаются от должности приказом генерального директора.

5. Основными структурными единицами предприятия являются отделы (цеха, участки (далее - отделы) предприятия).

Руководят работой отделов начальники отделов. Начальники отделов назначаются и освобождаются от должности приказом генерального директора предприятия по согласованию с главным инженером, заместителем генерального директора предприятия, курирующим структурное подразделение.

6. Для решения конкретных задач в составе отделов создаются дополнительные структурные единицы: участки (посты, бригады) (далее – участки).

Общее управление работой участков осуществляют начальники отделов. Непосредственно управляет работой участка мастер. Руководитель дополнительной структурной единицы назначается и освобождается от должности приказом генерального директора предприятия по согласованию с начальником отдела и заместителем генерального директора (Главным инженером).

Начальники технологических смен осуществляют свою деятельность во взаимодействии с руководителями структурных подразделений предприятия. Непосредственное руководство работой начальников технологических смен осуществляется начальником производственно-технического отдела.

Общее руководство работой начальников технологических смен осуществляет главный инженер.

7. Начальники технологических смен осуществляют руководство сотрудниками структурных подразделений предприятия, работающих в сменном режиме.

Административный персонал и структурные подразделения, непосредственное руководство которым осуществляет генеральный директор:

- Юрисконсульт;

- Отдел кадров;

- Секретарь руководителя;

- Инженер по техническому надзору;

- Инженер по ГО и ЧС;

- Мастер административно- хозяйственного участка;

- Производственная лаборатория:

В состав производственной лаборатории входит пост радиационного контроля;

- Администратор вычислительной сети.

|  |
| --- |
| Цех |
| Начальник цеха |
| Заместитель Начальника цеха по технической подготовке производства |
| Заместитель начальника цеха по производству |
| Участок |
| Начальник участка |
| Старший мастер |
| Мастер |
| Рабочая зона бригады |
| Бригадир |
| Рабочее место |
| рабочий |

Организационная структура цеха определяется типом производства, техническим уровнем и сложностью выпускаемой продукции, численностью рабочих, уровнем механизации и автоматизации производства и другими факторами, связанными с отраслевыми особенностями. При определении организационной структуры предприятий следует руководствоваться отраслевыми нормативами численности ИТР цехов основного и вспомогательного производства. На организационную структуру влияет степень централизации функций управления на данном предприятии. В зависимости от этого возможны примерные структуры цеха представлены на рисунке номер 4.

Рисунок 4. Структуры цеха

**Анализ положений о подразделениях**

ОАО "РОТ ФРОНТ" - это:

Один из крупнейших производителей и лидеров российского рынка; годовой выпуск более 50 тыс. тонн сладких изделий;

Сочетание новейших технологий с многолетними традициями производства высококачественной продукции.

Современное производство, оснащенное высокотехнологичным оборудованием от ведущих мировых производителей, на котором работают около 3000 высококвалифицированных сотрудников;

Натуральное сырье и экологическая чистота кондитерских изделий;

Высокое качество кондитерской продукции, подтвержденное Почетными Медалями, Призами и Дипломами отечественных и зарубежных выставок;

Более 200 наименований сладких изделий - карамели, конфет, шоколада, вафель, драже и халвы.

Конфеты составляют самую разнообразную группу. Они изготавливаются из различных конфетных масс: помадных, фруктовых, ореховых, сбивных, ликерных, грильяжных, пралиновых.

Наименование и место нахождения Общества

Фирменное наименование Общества на русском языке: полное - Открытое акционерное общество «РОТ ФРОНТ», сокращенное - ОАО «РОТ ФРОНТ».

Фирменное наименование Общества на английском языке: полное – Open-Type Joint Stock Company «ROT FRONT», сокращенное - ОJSC «ROT FRONT».

Место нахождения Общества: 113095 Москва, 2-й Новокузнецкий пер., д.13/15.****

Рисунок 5. Здание ОАО "РОТ ФРОНТ"

**2.2 Постановка задач**

Постановка задач в проектировании программной системы безопасности включает ряд ключевых задач, которые необходимо решить для обеспечения безопасности информации и защиты бизнес-процессов:

1. Идентификация и аутентификация пользователей: Задача состоит в создании механизмов и программных модулей, которые позволят идентифицировать и аутентифицировать пользователей, получающих доступ к информационной системе фирмы. Это включает, использование паролей, биометрических данных или других методов аутентификации.
2. Управление доступом: Основная задача заключается в определении и управлении правами доступа пользователей к различным ресурсам и функциональности информационной системы. Необходимо определить роли пользователей, установить гранулярные права доступа на основе принципа наименьших привилегий и разработать механизмы контроля доступа.
3. Защита данных: Важной задачей является обеспечение конфиденциальности, целостности и доступности данных фирмы. Необходимо разработать механизмы шифрования данных, контроля целостности данных, механизмы резервного копирования и восстановления данных, а также меры защиты от утечек данных или несанкционированного доступа.
4. Обнаружение и предотвращение инцидентов безопасности: Задача состоит в создании механизмов обнаружения и предотвращения возможных инцидентов безопасности, таких как взломы, атаки, вирусы и другие угрозы. Это может включать использование системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), механизмов мониторинга сетевого трафика и аудита действий пользователей.
5. Обучение и осведомленность пользователей: Задача заключается в проведении обучения сотрудников фирмы по вопросам безопасности информации. Это поможет повысить осведомленность сотрудников о потенциальных угрозах безопасности, принципах безопасного поведения, политиках паролей и правилах использования информационных ресурсов.
6. Системы мониторинга и реагирования: Задача состоит в разработке систем мониторинга и реагирования на возможные инциденты безопасности. Это может включать механизмы мониторинга сетевого трафика, журналов событий, системы уведомлений о нарушениях безопасности и процедуры реагирования на инциденты.
7. Внедрение и тестирование: Задача заключается в успешном внедрении разработанных программных средств безопасности в информационную систему фирмы. После внедрения необходимо провести тестирование системы на безопасность, чтобы убедиться в ее эффективности и надежности.

2.1 Разработка модели безопасности объекта

Модель безопасности объекта наглядно показывает способ обработки информации в случаи потенциальной опасности.

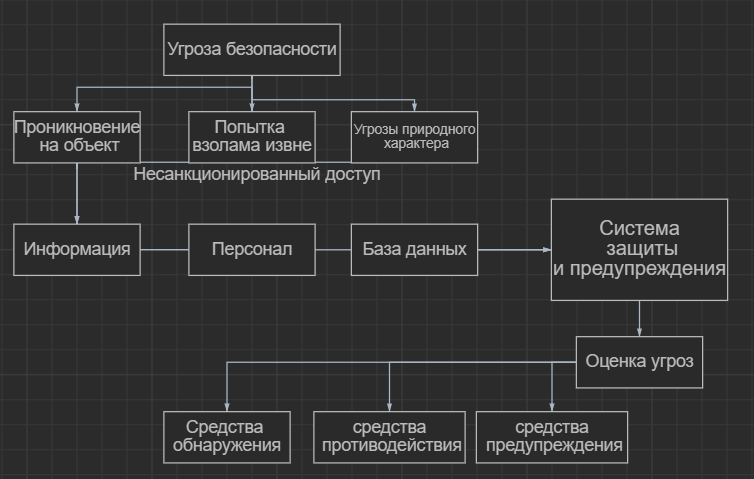


Рисунок 6. Модель безопасности объекта

Объекты первого класса защиты. К данным объектам защиты были отнесены все носители информации, уничтожение или хищение которых приведёт к остановке деятельности производства.

Объекты второго класса защиты. К данным объектам были отнесены объекты, уничтожение или хищение которых повлечёт осложнения в работе организации.

Объекты третьего класса защиты, к данным объектам были отнесены объекты, уничтожение или хищение которых незначительно скажется или никак не отразиться на деятельности фирмы.

Борьба с угрозами проходит в 4 этапа:

- Обнаружение угрозы;

- Определение вариантов реализации угрозы;

- Определение возможного ущерба от угрозы;

- Использование системы защиты от угрозы.

Система защиты от угроз включает в себя обнаружение, предотвращение и ликвидацию последствий.

2.2 Выбор средств и технологии для защиты объекта

Для достижения основной цели - обеспечения информационной безопасности необходимо решить следующие задачи:

Идентификация и аутентификация: Реализация механизмов идентификации и аутентификации позволит установить легитимность пользователей и контролировать доступ к информационной системе и ресурсам фирмы.

Управление доступом: Разработка системы ролей и привилегий для определения уровня доступа к различным ресурсам и функциональности системы. Роли могут включать администраторов, менеджеров, сотрудников и т.д.

Принцип наименьших привилегий: Применение принципа наименьших привилегий, при котором каждый пользователь получает только те привилегии, которые необходимы для выполнения своих задач.

Ограничение физического доступа: Обеспечение физической безопасности объекта путем установки физических барьеров, таких как замки, системы контроля доступа и видеонаблюдение, для предотвращения несанкционированного доступа к помещениям с важными ресурсами.

Мониторинг: Установка системы мониторинга и тревожной сигнализации, которая будет отслеживать активность и обнаруживать любые подозрительные или необычные события, такие как несанкционированный вход или попытки взлома.

Защита данных:

Шифрование данных: Применение шифрования данных при их хранении и передаче, чтобы обеспечить их конфиденциальность и предотвратить несанкционированный доступ.

Резервное копирование данных: Регулярное создание резервных копий данных, чтобы обеспечить возможность восстановления в случае потери данных из-за сбоев системы или кибератак.

Мониторинг и реагирование:

Системы мониторинга и регистрации событий: Установка системы мониторинга, которая будет отслеживать активность в информационной системе и регистрировать события для последующего анализа и обнаружения аномалий или атак.

Инцидентный менеджмент: Разработка процедур и планов реагирования на безопасностные инциденты, чтобы быстро и эффективно реагировать на возможные нарушения безопасности и минимизировать их последствия.

Обучение персонала: Обучение сотрудников фирмы основам безопасности информации, включая политики безопасности, процедуры аутентификации, правила обработки и хранения данных и распознавание социальной инженерии.

Осведомленность и культура безопасности: Создание культуры безопасности, включая поощрение сотрудников к активному участию в обеспечении безопасности, например, сообщение о подозрительных активностях или потенциальных рисках.

В настоящий момент в ОАО «Рот Фронт» используются следующие системы безопасности:

- видеонаблюдение

- система контроля доступа в помещения и офисы

- физическая охрана

Для обеспечения комплексной защиты необходимо усовершенствовать имеющиеся системы безопасности. Основные помещения, требующие дополнительные системы безопасности: кабинет директора, расположенный на третьем этаже здания, базы данных расположенные на первом этаже здания, бухгалтерия расположенная на третьем этаже здания.

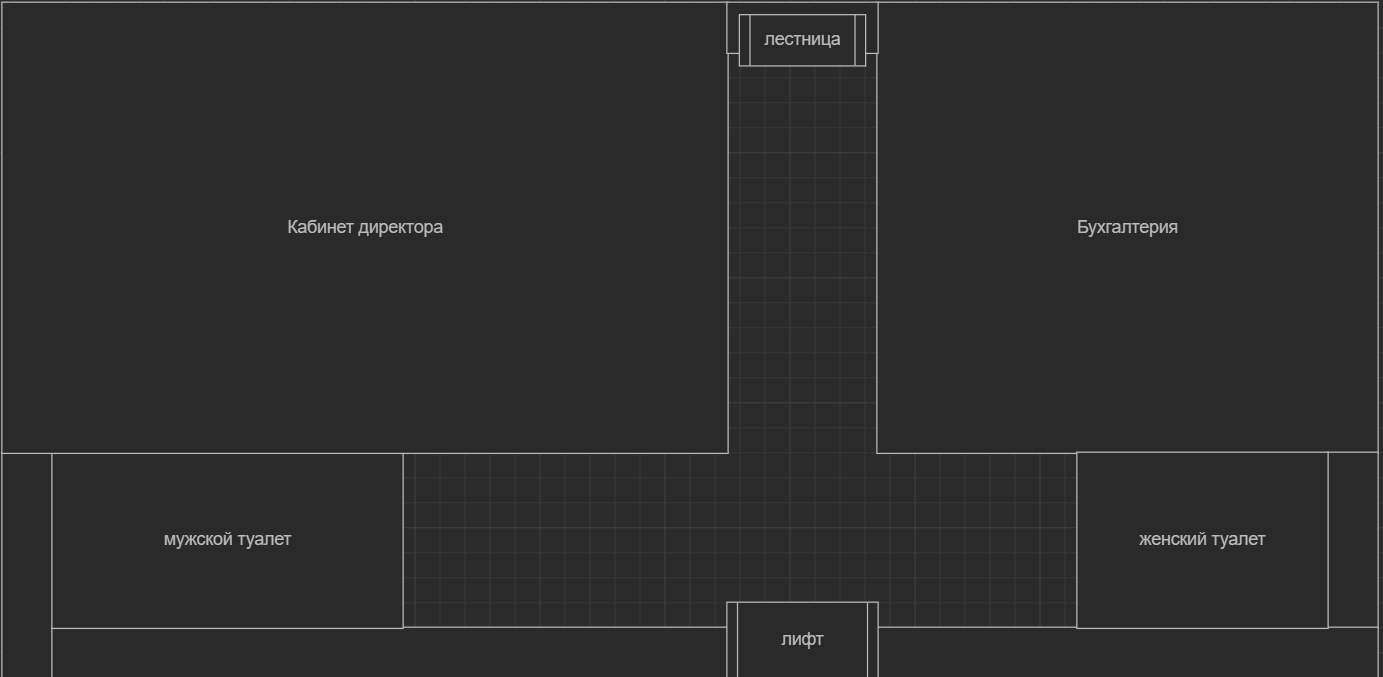


Рисунок 7. Третий этаж

В помещение находится одна камера видеонаблюдения, расположенная над выходом с лестницы на этаже, также используется система СКУД, для контроля доступа работников.

Этих мер безопасности недостаточно для защиты, так как злоумышленник может сломать камеру из неконтролируемой зоны, и для большей эффективности необходимо установить дополнительные технические средства защиты.

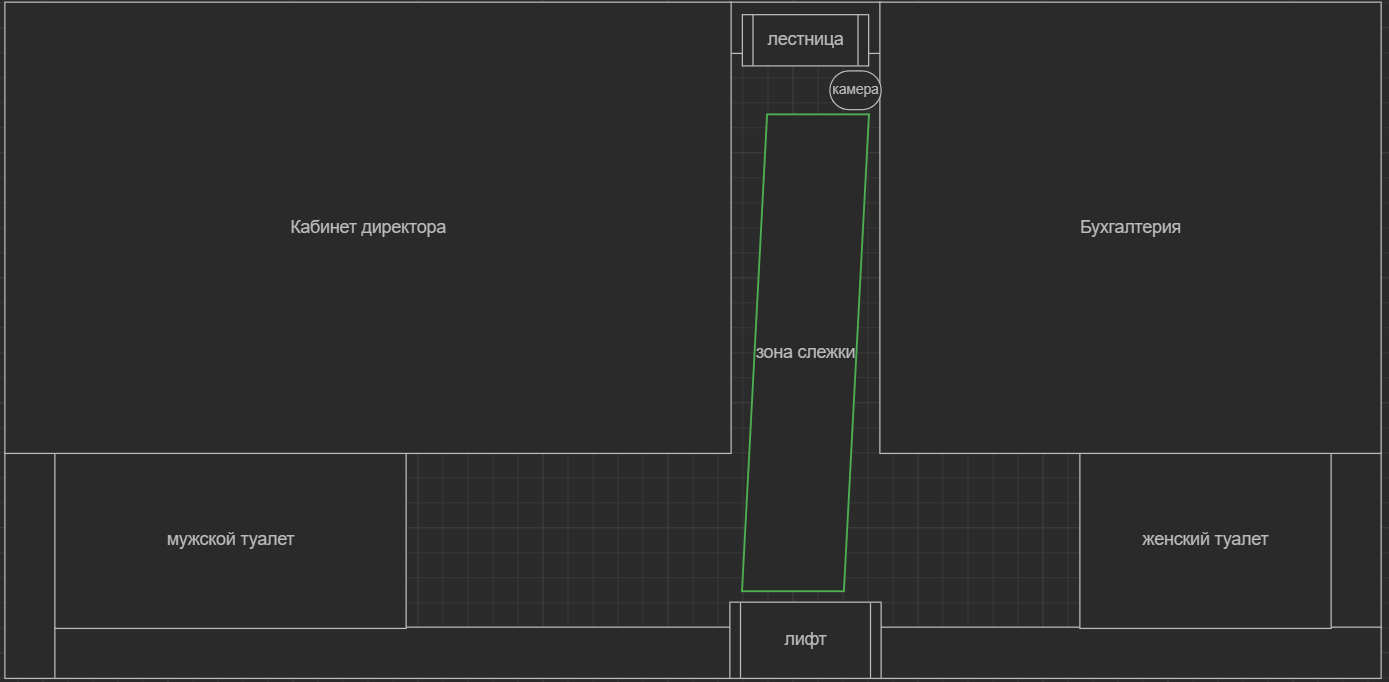


Рисунок 8. Третий этаж с камерой

Видеонаблюдение на этаже

Проведя анализ действующей на ОАО «Рот Фронт» системы защиты, сделан вывод о возможности проведения усовершенствования системы защиты, в частности установка дополнительных мер защиты отдельных помещений.

Так как существует большое количество зон, в которых осуществляется деятельность сотрудников организации и клиентов, не попадающих, или попадающих частично в контролируемую зону.

Необходимо оснастить дополнительным оборудованием коридор.

Задачи, которые будут решены дооснащением:

- Своевременное обнаружение,

- Контроль,

- Защита от несанкционированного доступа.

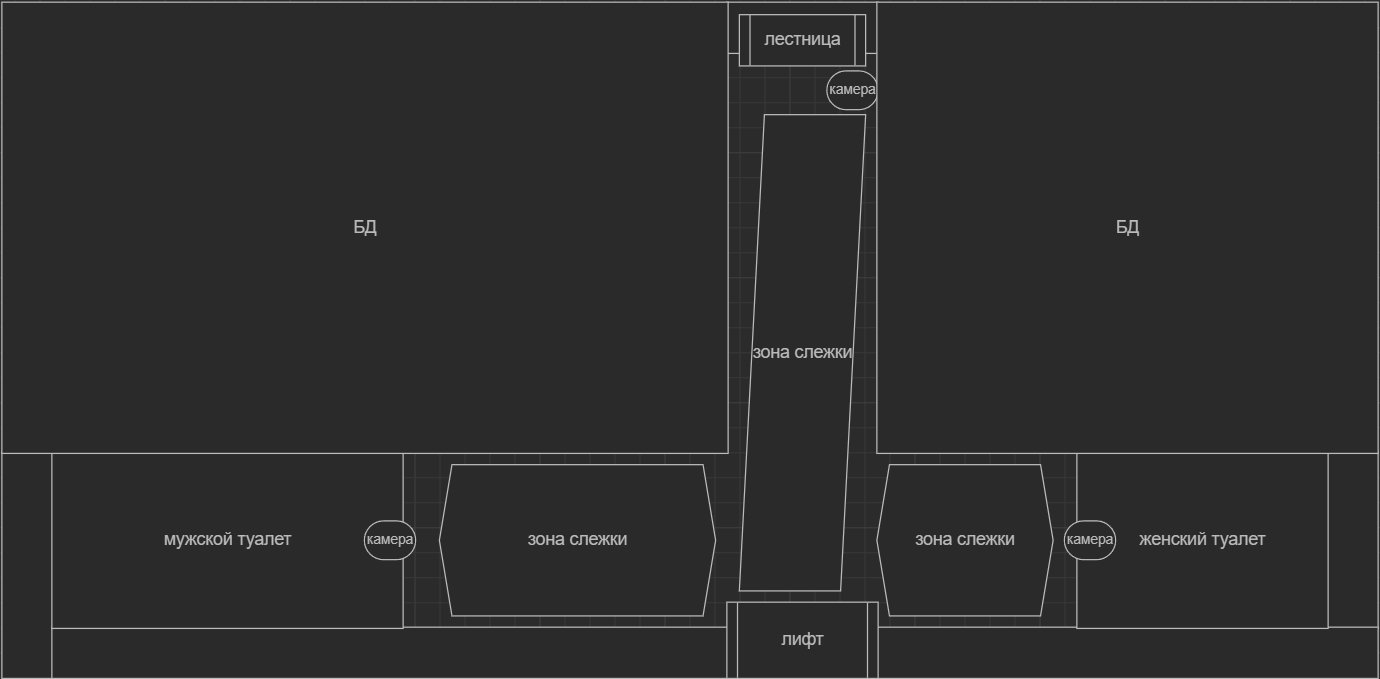


Рисунок 9. Первый этаж

На первом этаже расположено 3 камеры видеонаблюдения, доступ к БД контролируется системой СКУД.

Внутри помещения с БД находятся датчики присутствия.

На предприятии ОАО «Рот Фронт» используется Ленточное резервное хранилище.



Рисунок 9. Ленточное резервное хранилище

Для оптимизации хранилища, целесообразней использовать облачное хранилище данных.

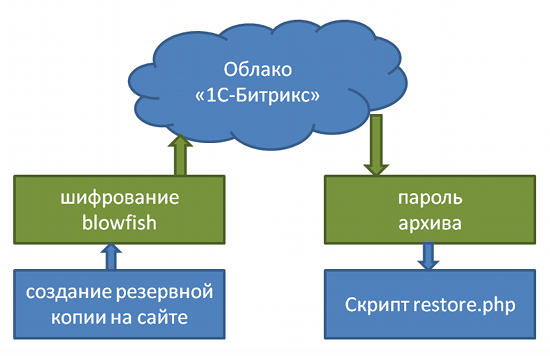


Рисунок 10. Облачное хранилище данных

Для защиты данных использованы системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS).

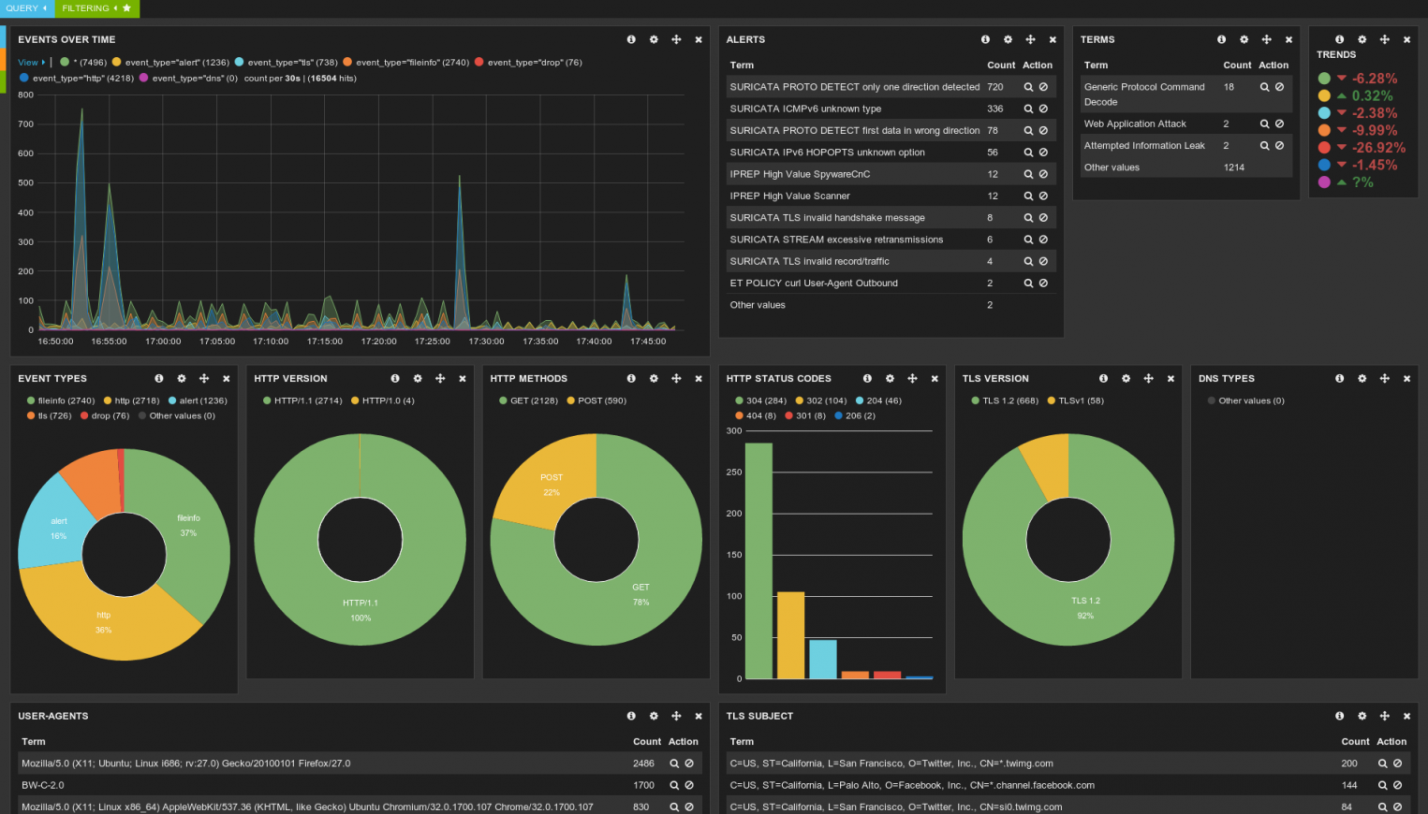


Рисунок 11. Системы предотвращения вторжений

Фото с экрана системы обнаружения и предотвращения вторжений на ОАО «Рот Фронт»

Шифрование данных на предприятии ОАО «Рот Фронт» не используется.

Для улучшения защиты нужно внедрить алгоритмы шифрования, к примеру Advanced Encryption Standard.

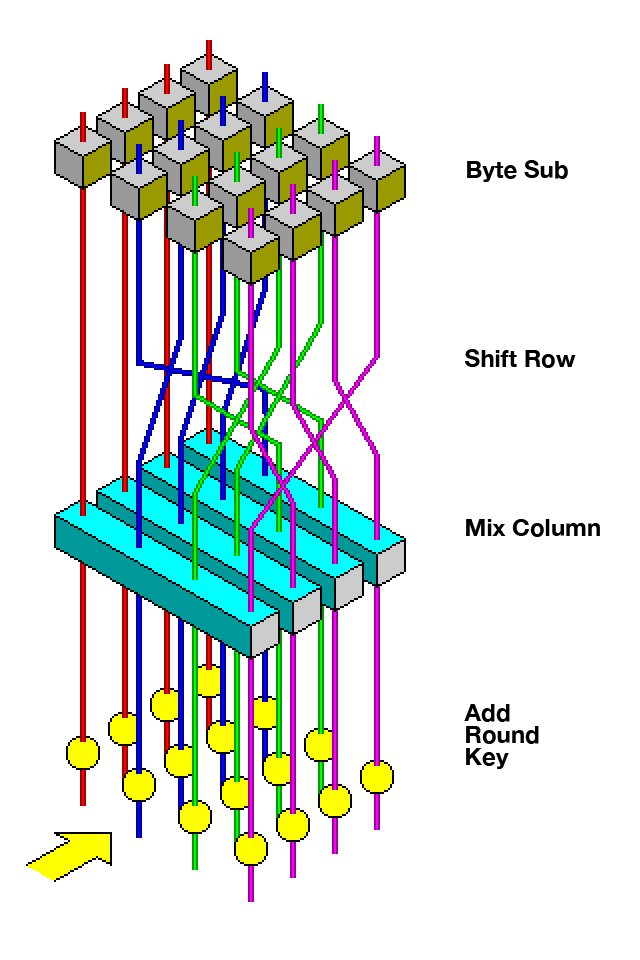


Рисунок 12. Алгоритмы шифрования

Byte sub – первоначальная структура

Shift row – сдвиг

Mix column – раздел перемешивания

Add Round key – добавление ключей

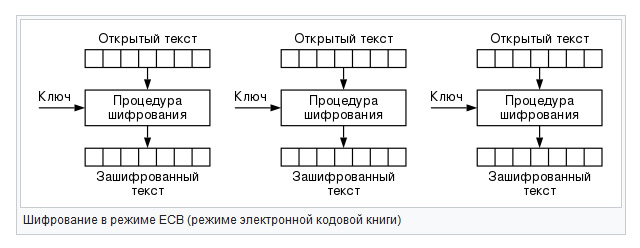


Рисунок 13. Схема алгоритма шифрования

На предприятии ведется обучение по правильной обработке и хранению данных, процедурам резервного копирования и использованию данных.

**2.4 Комплекс организационно-технических мероприятий по внедрению предложенных решений**

Пример реализации облачного хранилища данных для может включать следующие шаги и компоненты:

Выбор облачного провайдера: внедрение облачного провайдера, такого как Amazon Web Services (AWS), Microsoft Azure или Google Cloud, с соответсвенными требованиями по безопасности, масштабируемости и доступности.

Создание облачного аккаунта: регистрация на выбранном облачном провайдере и создание аккаунт предприятия.

Определение требований к хранилищу данных: это могут быть рецепты, заказы, инвентарные данные, финансовая информация и т.д.

Настройка безопасности: Внедрение соответствующих мер безопасности в облачное хранилище данных:

Аутентификация и авторизация: нужно, чтобы только авторизованные пользователи имели доступ к конкретным данным.

Шифрование данных: Использование алгоритмов шифрования данных при их хранении и передаче, чтобы обеспечить конфиденциальность.

Обнаружение и предотвращение угроз: реализовать механизм обнаружения и предотвращения угроз, такие как мониторинг сетевой активности и применение механизмов защиты от вредоносного ПО.

Резервное копирование и восстановление данных: установка регулярного резервного копирования данных, и выбор плана по восстановлению.

Организация структуры хранения данных: создать структуру хранения данных в облачном хранилище, которая будет соответствовать потребностям фирмы. Разделите данные на категории, установить права доступа к каждой категории и определите стандарты и правила именования файлов и папок.

Интеграция существующих систем: Внутренние информационные системы, такие как система учета или система управления заказами, интегрируется между облачным хранилищем данных. Это позволит автоматизировать передачу данных и обеспечит актуальность и согласованность информации.

Обучение персонала: обучить сотрудников производства правилам использования облачного хранилища данных, включая доступ, резервное копирование и восстановление данных, обработку конфиденциальных информаций и соблюдение политик безопасности.

Реализовать систему мониторинга для отслеживания активности в облачном хранилище данных, и систему обнаружения аномалий и предотвращения возможных угроз.

Пример реализации шифрования данных для может включать следующие шаги:

Определение типов данных для шифрования: определите, какие типы данных требуют шифрования. Например, это могут быть финансовые данные, персональные данные клиентов или рецепты.

Выбор алгоритма шифрования: например, AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) или Blowfish, и выбрать тот, который наилучшим образом реализует потребности безопасности и производительности.

Разработка системы ключей: создать систему управления ключами для шифрования и расшифровки данных. Это может включать генерацию и управление секретными ключами, а также их распределение и хранение.

Интеграция шифрования в приложения и базы данных: внедрить шифрование данных в приложения и базы данных предприятия. Обычно это требует изменений в коде приложений или использования специальных функций и API для шифрования и расшифровки данных.

Управление ключами: обеспечить безопасное управление ключами шифрования. Это может включать хранение ключей в защищенном хранилище, установку политик доступа к ключам и регулярное обновление ключей для обеспечения безопасности данных.

Пример реализации обучения персонала по правилам безопасности и защите данных для предприятия включает следующие шаги:

Обучение персонала: обучение сотрудников предприятия правилам использования шифрования данных. Обучение особенностям работы с зашифрованными данными, Объяснение необходимости сохранения ключей в безопасности.

Мониторинг и аудит шифрования: Внедрение системы мониторинга шифрования, которая будет отслеживать использование шифрования данных и предупреждать об аномалиях или возможных нарушениях безопасности. Проводить регулярные аудиты шифрования, чтобы проверить эффективность и соответствие шифрования требованиям безопасности.

Пример реализации обучения персонала по правилам безопасности и защите данных на предприятии может включать следующие шаги:

Идентификация необходимых навыков: определение навыков и знаний, необходимых сотрудникам для обеспечения безопасности данных. Это может включать понимание основных принципов безопасности, процедур доступа, резервного копирования и восстановления данных, а также обработки конфиденциальных информаций.

Разработка программы обучения: создать структурированную программу обучения, которая позволит сотрудникам ознакомиться с конкретными политиками безопасности фирмы. Включить в нее как теоретическую часть, так и практические упражнения.

Обучение на рабочем месте: предоставить сотрудникам обучение на рабочем месте, чтобы они могли применять полученные знания и навыки непосредственно в своей работе. Например, проводите тренировки по правильной обработке и хранению данных, процедурам резервного копирования или использованию безопасных паролей.

Постоянное обновление: обеспечить постоянное обновление, обучения сотрудников, чтобы они могли быть в курсе новых угроз безопасности и изменений в политиках и процедурах безопасности данных. Проводите регулярные обучающие сессии или предоставляйте доступ к онлайн-ресурсам и материалам по безопасности данных.

Контроль и оценка: установить механизмы контроля и оценки эффективности обучения. Это может включать тестирование знаний сотрудников, оценку их способности применять полученные знания на практике и обратную связь для улучшения обучающих программ.

Информационные материалы: подготовить информационные материалы, которые можно распространить сотрудникам для дополнительного ознакомления с правилами безопасности и рекомендациями по защите данных. Это могут быть брошюры, постеры, электронные ресурсы или внутренний портал с информацией о безопасности.

Ролевые игры и симуляции: использовать ролевые игры и симуляции, чтобы сотрудники могли в практической среде понять важность соблюдения правил безопасности и осознать последствия нарушений.

Награды и поощрения: нужно создать систему поощрения и награждения сотрудников, которые активно принимают участие в обучении и соблюдают правила безопасности данных. Это может быть в форме похвалы, бонусов или премий.

Важно создать культуру безопасности данных внутри организации и обеспечить постоянное внимание к обучению персонала по этой теме. Это поможет минимизировать риски нарушения безопасности данных и защитить кондитерскую фирму от потенциальных угроз.

Реализация всех пунктов позволит решить следующие задачи:

Создание системы безопасности позволит обеспечить конфиденциальность данных фирмы, предотвращая несанкционированный доступ к ним.

Реализация системы безопасности позволит обнаруживать и предотвращать попытки несанкционированного изменения данных, обеспечивая их целостность.

Программные средства защиты будут обеспечивать мониторинг и обнаружение попыток атак и вторжений в систему, а также принимать меры для предотвращения их успеха.

Облачные средства хранения будут обеспечивать резервное копирование данных и возможность восстановления в случае сбоев или потери информации.

Реализация системы безопасности будет включать обучение сотрудников по правилам безопасности и осведомление их о существующих угрозах и процедурах защиты данных.

Программная система безопасности будет разработана с учетом соответствия нормативным требованиям и стандартам безопасности данных, что поможет соблюдать законодательство и регулятивные нормы.

Реализация системы безопасности позволит осуществлять мониторинг и аудит безопасности системы, что позволит выявлять потенциальные нарушения и обеспечивать соответствие установленным правилам и политикам безопасности.

Программная система безопасности должна быть гибкой и поддерживать постоянное развитие, чтобы адаптироваться к новым угрозам и технологическим изменениям в области информационной безопасности.

Реализация всех этих задач поможет создать надежную и безопасную среду для хранения и обработки данных ОАО «РОТ ФРОНТ», а также защитит ее от потенциальных угроз и рисков.

**ЗАКЛЮЧЕНИЕ**

В ходе проведения исследования и разработки программной системы безопасности для кондитерской фирмы ОАО «Рот Фронт» были достигнуты следующие результаты.

Был проведен анализ требований безопасности кондитерской фирмы. Идентифицированы уязвимости и потенциальные угрозы безопасности, а также определены требования к конфиденциальности, целостности и доступности данных. Были изучены правовые и нормативные аспекты, чтобы обеспечить соответствие системы безопасности требованиям законодательства.

Была разработана программная система безопасности, включающая выбор подходящих программных средств защиты. Была создана модель безопасности объекта, определены мероприятия для защиты базы данных и реализовано облачное хранилище данных. Эти шаги обеспечивают надежное хранение и обработку информации, а также защиту от потенциальных угроз и рисков.

Был реализован механизм шифрования данных. Были изучены методы и алгоритмы шифрования. Путем реализации шифрования данных была обеспечена дополнительная защита конфиденциальности информации, предотвращая несанкционированный доступ к ней.

Был проведен процесс обучения персонала по правилам безопасности данных. Разработан и предложен план обучения. Это позволило повысить осведомленность сотрудников о безопасности данных и уменьшить вероятность возникновения ошибок или небрежного обращения с информацией.

Итоговые рекомендации и выводы основаны на проведенном исследовании и реализации программной системы безопасности для кондитерской фирмы. Данная система позволяет эффективно защищать данные и обеспечивать безопасную среду для работы с информацией. Она способствует укреплению конфиденциальности, целостности и доступности данных, а также снижает риск возникновения угроз безопасности и нарушений информационной безопасности.

В заключение, реализация программной системы безопасности является важным шагом в обеспечении защиты данных и информационной безопасности. Она позволяет снизить риски, связанные с угрозами безопасности, и обеспечить надежность работы с конфиденциальными данными. Применение разработанных рекомендаций и мероприятий, представленных в данной работе, будет способствовать эффективной защите кондитерской фирмы от внешних и внутренних угроз безопасности данных.

**СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости. Москва, 2009.
2. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
3. ФСТЭК: Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).
4. В.Ф. Шаньгин – Информационная безопасность компьютерных систем и сетей, Москва, ИД «ФОРУМ» - ИНФРА-М, 2008 г.
5. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г., 28 июня, 27 июля, 29 ноября, 23 декабря 2010 г.).
6. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных; Учебник для высших учебных заведений / Под ред. проф. А.Д. Хомоненко. - 4-е изд., доп. и перераб. - СПб.: КОРОНА принт, 2004. - 736 с. ISBN 5‑7931‑0284‑1.
7. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. Волгоград: Изд-во ВолГУ, 2002. – 122с. – (Серия «Информационная безопасность»). ISBN 5-85534-640-4.
8. ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения.
9. Гагарина Л.Г., Кокорева Е.В., Виснадул Б.Д. Технология разработки программного обеспечения. - М.: ИД «ФОРУМ»; ИНФРА-М, 2008. - ISBN 978-5-8199-0342-1.
10. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2.
11. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2004. - 544 с. ISBN 5-8291-0408-3.
12. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288 с: ил. ISBN 5-94157-331-6.
13. Э. Мэйволд – Безопасность сетей [Электронный ресурс] – Режим доступа: <http://www.intuit.ru/department/security/netsec/11/1.html>.
14. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г., 28 июня, 27 июля, 29 ноября, 23 декабря 2010 г.).
15. Информационный бюллетень Jet Info №5 (192)/2009.
16. Братищенко В.В. Проектирование информационных систем. - Иркутск: Изд-во БГУЭП, 2004. - 84 с.
17. Сивидов К.В. Проектирование и создание чего-то прекрасного из звуков. – Москва: Изд-во Moon, c 2004г.
18. Введение в SSL [Электронный ресурс] – Режим доступа: <https://developer.mozilla.org/en/Introduction_to_SSL>
19. Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley
20. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. - 316 с.
21. Chapple, M., & Seidl, T. (2019). CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. Sybex.