ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Уральский государственный университет путей сообщения»

**КУРСОВОЙ ПРОЕКТ ПО ТЕМЕ «**Разработка организационной модели защиты информации на предприятии»

по дисциплине «Организационное и правовое обеспечение

информационной безопасности»

Проверил Выполнил:

Преподаватель: студент гр. ИБ-321

Чукалова Л.Г Мишагин Г.Ю.

Екатеринбург

2024

**Оглавление.**

|  |  |
| --- | --- |
| Введение……………………………………………………………………. | 3 |
| Цель…………………………………………………………………………. | 4 |
| 1 Изучение организационной модели защиты информации на предприятии……. | 5 |
| 2 Разработка организационной модели защиты информации на предприятии…... | 7 |
| Заключение…………………………………………………………………. | 10 |
| Список источников………………………………………………………… | 11 |

**Введение.**

Современное предприятие сталкивается с постоянно растущей угрозой кибератак и утечек конфиденциальной информации, что подчеркивает актуальность внедрения эффективных систем защиты информации. В контексте развивающихся технологий и расширяющейся цифровой среды, обеспечение безопасности данных на предприятии становится неотъемлемой частью стратегии управления. Данный проект направлен на разработку организационной модели защиты информации, которая не только соответствует современным стандартам и требованиям безопасности, но и адаптируется к уникальным особенностям и потребностям конкретного предприятия.

В ходе исследования будут рассмотрены ключевые аспекты, влияющие на эффективность системы защиты информации на предприятии, такие как человеческий фактор, технологическая инфраструктура, процессы управления безопасностью и соответствие нормативным требованиям. Результаты работы могут послужить основой для разработки конкретных рекомендаций и решений, направленных на повышение уровня безопасности информации на предприятии в современной цифровой среде.

**Цель.**

Целью данной курсовой работы является предложение эффективной и интегрированной модели защиты информации на предприятии, способной минимизировать риски утечек, несанкционированного доступа и других киберугроз. Для достижения этой цели предполагается провести анализ существующих методов и подходов к защите информации, выделить основные уязвимости и риски, а также разработать систему мер, ориентированных на создание устойчивой и надежной системы информационной безопасности.

**1 Изучение организационной модели защиты информации на предприятии.**

Организация защиты информации на предприятии (ОрЗИ) является важнейшей составляющей разработки системы защиты информации на предприятии. Однако, существующие модели ОрЗИ в недостаточной мере четко и ясно формируют представление о ее структуре, составе и содержании, что создает серьезную проблематику обеспечения информационной безопасности организации. В связи с этим, в целях повышения эффективности обеспечения информационной безопасности организации очевидна постановка задачи о разработке модели организации защиты информации на предприятии. В соответствии с ГОСТ Р 50922-2006 (ГОСТ) Система зашиты информации (СЗИ) определяется как совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.  
Организационная защита информации — это комплекс мер и мероприятий, направленных на обеспечение безопасности информационных ресурсов организации. Она включает в себя следующие аспекты:

1. Разработка политики информационной безопасности:

- Определение целей и задач защиты информации;

- Установление правил и норм использования информационных систем и ресурсов;

- Разработка процедур контроля доступа к информации.

2. Создание структуры управления безопасностью:

- Назначение ответственных за безопасность информации;

- Формирование подразделений или служб, занимающихся защитой информации.

3. Обучение и повышение квалификации персонала:

- Проведение тренингов и семинаров по вопросам безопасности информации;

- Повышение осведомлённости сотрудников о возможных угрозах и мерах защиты.

4. Контроль и аудит безопасности:

- Регулярное проведение проверок соблюдения политики безопасности;

- Анализ инцидентов и выявление уязвимостей системы защиты.

5. Обеспечение физической безопасности:

- Защита помещений, где расположены информационные ресурсы;

- Контроль доступа к оборудованию и носителям информации.

6. Использование технических средств защиты:

- Установка антивирусного ПО, межсетевых экранов, систем обнаружения вторжений и других технических решений;

- Обеспечение резервного копирования данных.

7. Взаимодействие с правоохранительными органами:

- Сотрудничество с органами внутренних дел для расследования инцидентов информационной безопасности.

8. Мониторинг и анализ угроз:

- Постоянное отслеживание новых видов киберугроз и методов их предотвращения.

9. Управление рисками:

- Оценка рисков информационной безопасности и разработка мер по их снижению.

Организационная защита информации является ключевым элементом общей системы безопасности предприятия. Её эффективность зависит от чёткого понимания целей и задач, а также от слаженной работы всех участников процесса обеспечения безопасности.

В ГОСТе разъяснений в отношений составляющей СЗИ «организованная» нет. Вместе с этим, в целом ряде законодательных и нормативно-правовых документов РФ в области защиты информации содержатся определенные подходы к формированию состава и содержания мер по организации защиты информации. Наиболее ёмко и концентрированно это изложено в пункте 1 статьи 16 Федерального закона «Об информации, информационных технологиях и о защите информации» следующим образом:

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Ключевым в этом случае является – …принятие правовых, организационных и технических мер…, однако не раскрывающим в полной мере структуру, состав, содержание и взаимосвязь составляющих организации защиты информации на предприятии.

На основе анализа законодательных и нормативно-правовых документов РФ в области защиты информации было принято решение использовать для основы разработки модели ОрЗИ моделирование взаимосвязи видов и направлений защиты информации.

Виды ЗИ в соответствии с ГОСТ Р 50922 определяются следующим образом:

- правовая защита информации: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

- техническая защита информации; ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- криптографическая защита информации: Защита информации с помощью ее криптографического преобразования;

- физическая защита информации: Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

**2 Разработка организационной модели защиты информации на предприятии.**

При этом, в практическом, плане каждый из видов ЗИ взаимосвязан с любым другим. Так, к примеру, техническая ЗИ предусматривает установление контролируемой зоны (КЗ), что является элементом физической ЗИ. При этом установление КЗ оформляется соответствующим актом, что, в свою очередь, является элементом правовой ЗИ, или, точнее - организационно-правовой ЗИ на предприятии (это очевидно, т.к. любое организационное мероприятие в рамках предприятия обязано быть подтверждено в соответствующем документальным порядке).

С системных позиций концепт модели взаимосвязи видов защиты информации может быть представлен следующим образом:

|  |  |
| --- | --- |
| Организационно - правовая ЗИ | Техническая ЗИ |
| Криптографическая ЗИ | Физическая ЗИ |

Таблица 1 - Концепт модели взаимосвязи видов защиты информации

Направления ЗИ сформированы в известной модели защиты информации, концепт которой представлен на рисунке 1:

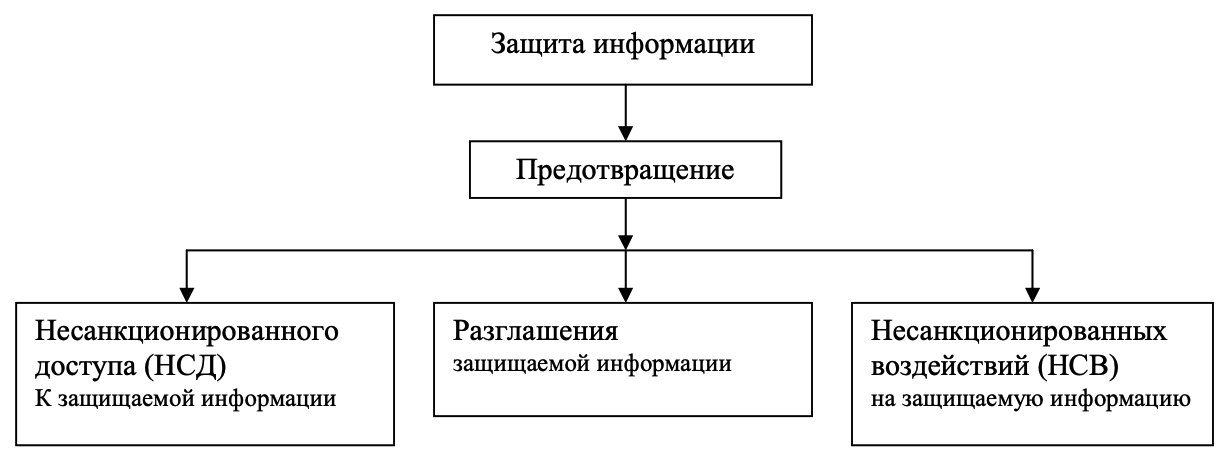


Рисунок 1. Концепт модели защиты информации

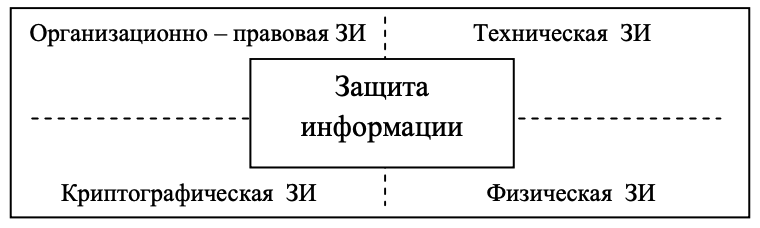
Изложенное позволяет представить концепт модели ОрЗИ следующим образом: 

Рисунок 2. Концепт модели взаимосвязи видов защиты информации

А также определить, что организация защиты информации осуществляется по совокупности и взаимосвязи всех видов и направлений защиты информации.

Это позволяет представить финальный вариант модели ОрЗИ в следующем виде:

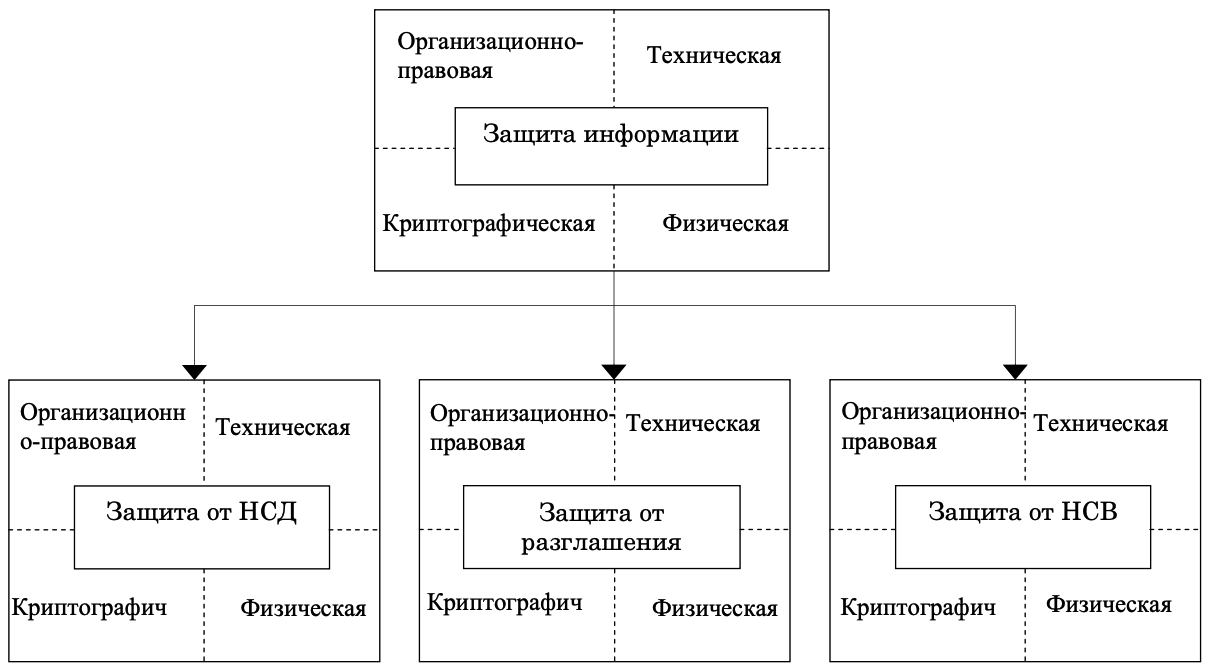


Рисунок 3. Модель организации защиты информации на предприятии

**Заключение.**

В современном информационном обществе, где технологические инновации и цифровая трансформация играют ключевую роль в деятельности предприятий, обеспечение надежной защиты информации становится неотъемлемой составляющей успешного управления. Данная курсовая работа посвящена разработке организационной модели защиты информации на предприятии, и ее целью было предложение системного и эффективного подхода к обеспечению безопасности данных.

В ходе исследования были рассмотрены существующие методы и подходы к защите информации. Акцент сделан на важности учета человеческого фактора, технологической инфраструктуры, процессов управления безопасностью и соответствия нормативным требованиям.

Разработанная организационная модель представляет собой комплексный подход, направленный на минимизацию рисков утечек и несанкционированного доступа. Внедрение предложенных рекомендаций позволит предприятию не только повысить уровень защиты информации, но и создать устойчивую систему информационной безопасности, гармонично взаимодействующую с основными бизнес-процессами.

В заключение можно отметить, что обеспечение информационной безопасности – это постоянный и динамичный процесс, требующий не только внедрения передовых технологий, но и постоянного мониторинга, обновления стратегий и обучения персонала. Разработанная модель представляет собой основу для дальнейших исследований и практической реализации в области информационной безопасности предприятия, учитывая его специфику и особенности.

**Список источников.**

1. ГОСТ Р 50922-2006 ''Защита информации. Основные термины и определения''.

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

3. ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ МЕТОДИЧЕСКИЙ ДОКУМЕНТ МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4. КонсультантПлюс - законодательство РФ кодексы и законы в последней редакции. <https://www.consultant.ru/document/cons_doc_LAW_61798/0e9ec16b786dcbdaaa7f44abfc4a15e601d5be22/>

5. Защита информации в нормах федерального закона Российской Федерации

<https://cyberleninka.ru/article/n/zaschita-informatsii-v-normah-federalnogo-zakona-rossiyskoy-federatsii>

6.ГАРАНТ-Законодательство(кодексы,законы,указы): [http://ivo.garant.ru/#%2Fbasesearch%2F1%20статьи%2016%20Федерального%20закона%20«Об%20информации%2C%20информационных%20технологиях%20и%20о%20защите%20информации»%2Fall%3A1](http://ivo.garant.ru/%23/basesearch/1%2520%25D1%2581%25D1%2582%25D0%25B0%25D1%2582%25D1%258C%25D0%25B8%252016%2520%25D0%25A4%25D0%25B5%25D0%25B4%25D0%25B5%25D1%2580%25D0%25B0%25D0%25BB%25D1%258C%25D0%25BD%25D0%25BE%25D0%25B3%25D0%25BE%2520%25D0%25B7%25D0%25B0%25D0%25BA%25D0%25BE%25D0%25BD%25D0%25B0%2520%25C2%25AB%25D0%259E%25D0%25B1%2520%25D0%25B8%25D0%25BD%25D1%2584%25D0%25BE%25D1%2580%25D0%25BC%25D0%25B0%25D1%2586%25D0%25B8%25D0%25B8,%2520%25D0%25B8%25D0%25BD%25D1%2584%25D0%25BE%25D1%2580%25D0%25BC%25D0%25B0%25D1%2586%25D0%25B8%25D0%25BE%25D0%25BD%25D0%25BD%25D1%258B%25D1%2585%2520%25D1%2582%25D0%25B5%25D1%2585%25D0%25BD%25D0%25BE%25D0%25BB%25D0%25BE%25D0%25B3%25D0%25B8%25D1%258F%25D1%2585%2520%25D0%25B8%2520%25D0%25BE%2520%25D0%25B7%25D0%25B0%25D1%2589%25D0%25B8%25D1%2582%25D0%25B5%2520%25D0%25B8%25D0%25BD%25D1%2584%25D0%25BE%25D1%2580%25D0%25BC%25D0%25B0%25D1%2586%25D0%25B8%25D0%25B8%25C2%25BB/all:1)