

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

# РТУ МИРЭА

**Колледж программирования и кибербезопасности**

Отчет о выполнении практического задания

по дисциплине «Программные и программно-аппаратные средства защиты информации»

на тему «Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите

информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов»

Практическое задание № 1

Специальность – 10.02.05 Информационная безопасность автоматизированных систем

Выполнил студент: Рунов К.С

Группа: ИБ-31

Руководитель: Журавлева В. С.

Работа защищена с оценкой \_\_\_\_\_\_\_\_\_\_

Москва

2024

**Введение**

Целью данной работы является проведение анализа нормативных правовых актов и методических документов, регламентирующих защиту информации с использованием программных и программно-аппаратных средств. Это включает изучение основных требований и рекомендаций, содержащихся в федеральных законах, приказах ФСТЭК и ФСБ России, а также в государственных стандартах. Анализ направлен на выявление ключевых положений, необходимых для обеспечения безопасности данных в информационных системах, а также на понимание применения этих нормативов на практике.

**Теоретические вопросы:**

1. Программно-аппаратная защита информации - это комплекс мер и технологий, направленных на обеспечение безопасности информационных систем и данных. Она включает в себя как программные, так и аппаратные компоненты, которые объединяются для защиты от различных угроз и атак.

Основными задачами программно-аппаратной защиты информации являются:

1. Защита от несанкционированного доступа - предотвращение проникновения злоумышленников в информационную систему или нарушения конфиденциальности данных.
2. Защита от вредоносного программного обеспечения - обнаружение и блокирование вирусов, троянских программ, шпионских программ и других вредоносных атак.
3. Защита данных - шифрование и защита информации от утечки или уничтожения.
4. Мониторинг и обнаружение инцидентов безопасности - поиск и анализ аномалий в работе информационной системы для своевременного реагирования на угрозы.
5. Управление доступом - установление правил и политик доступа к данным и ресурсам, контроль привилегий пользователей.
6. Резервное копирование и восстановление данных - создание резервных копий для предотвращения потери информации в случае аварий, а также восстановление данных при необходимости.
7. Основные понятия программно-аппаратной защиты информации:
8. Информационная безопасность — защита информации и поддерживающих ее систем от несанкционированного доступа, раскрытия, изменения, уничтожения или нарушения доступности.
9. Конфиденциальность — свойство информации, при котором доступ к ней ограничен для неавторизованных лиц или систем.
10. Целостность — свойство информации сохранять свою точность и полноту, защищенность от несанкционированных изменений.
11. Доступность — обеспечение возможности получения информации или использования ресурсов, когда это необходимо уполномоченным лицам или системам.
12. Аутентификация — процесс проверки подлинности пользователя или системы, который осуществляется с помощью паролей, биометрии, сертификатов и других методов.
13. Авторизация — процесс предоставления пользователю прав на выполнение определенных действий или доступ к ресурсам на основе его уровня доступа.
14. Шифрование — процесс преобразования информации в нечитабельный формат для защиты данных от несанкционированного доступа. Для восстановления исходных данных используется ключ расшифровки.
15. Файервол — программное или аппаратное средство, фильтрующее входящий и исходящий трафик между сетями с целью предотвращения несанкционированного доступа.
16. Антивирусное программное обеспечение — программы, предназначенные для обнаружения, блокировки и устранения вредоносного кода, такого как вирусы, трояны и черви.
17. IDS/IPS (системы обнаружения и предотвращения вторжений) — программные или аппаратные средства, которые отслеживают сетевой трафик или системные события для выявления потенциальных атак или аномалий и блокировки их.
18. Защита на уровне операционной системы — использование встроенных механизмов безопасности операционных систем, таких как контроль доступа, разграничение прав пользователей и шифрование.
19. Аппаратные средства защиты — устройства, которые обеспечивают безопасность на физическом уровне (например, смарт-карты, токены, аппаратные модули безопасности).
20. Многофакторная аутентификация (MFA) — метод защиты, требующий от пользователя предоставления двух или более видов подтверждения для получения доступа к системе.
21. Системы резервного копирования — средства, обеспечивающие сохранение и восстановление данных в случае их утраты или повреждения.
22. Методы защиты информации можно классифицировать следующим образом:

По уровню защиты:

- Физическая защита: защита оборудования и помещений (замки, охрана, видеонаблюдение).

- Логическая защита: программные средства защиты (антивирусы, системы обнаружения вторжений).

По типу угроз:

- Превентивные меры: предотвращение угроз (шифрование, контроль доступа).

- Реакция на инциденты: меры по восстановлению после инцидента (резервное копирование, восстановление данных).

По способу реализации:

- Программные средства: антивирусные программы, фаерволы, системы управления доступом.

- Аппаратные средства: шифраторы, токены, смарт-карты.

По области применения:

- Корпоративная защита: системы защиты для организаций и предприятий.

- Персональная защита: средства защиты для индивидуальных пользователей.

По степени автоматизации:

- Автоматизированные системы защиты: полностью автоматические решения (например, IDS/IPS).

- Полуавтоматизированные системы: требуют вмешательства человека (например, ручная проверка логов)

**4.** Нормативно-правовые акты и документы по защите информации

1. Конституция Российской Федерации

Конституция РФ, как основной закон страны, закладывает фундаментальные права и свободы граждан, включая защиту личной информации.

Статья 23: гарантирует право на неприкосновенность частной жизни, личную и семейную тайну. Это создает правовые основы для защиты персональных данных граждан и регулирует сбор, хранение и использование информации.

Статья 24: устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни граждан без их согласия. Это положение является ключевым для защиты конфиденциальной информации.

Статья 29: предоставляет право на свободный поиск, получение, передачу и распространение информации, а также запрет на цензуру. Важным аспектом является защита права на информацию в соответствии с нормами права.

2. Гражданский кодекс Российской Федерации

Гражданский кодекс РФ регулирует имущественные и личные неимущественные отношения, в том числе касающиеся информационных технологий и защиты информации.

Статья 128: определяет информацию как объект гражданских прав. Это означает, что информация может быть предметом правового регулирования, как и любое другое имущество.

Статья 139: регулирует вопросы защиты коммерческой тайны. Это информация, которая не подлежит раскрытию и требует специальной защиты. Организации обязаны применять меры по предотвращению утечек информации, используя как организационные, так и технические средства защиты.

Статья 150: регулирует защиту личной информации как нематериального блага, что создает правовые основы для защиты персональных данных граждан.

3. Уголовный кодекс Российской Федерации

Уголовный кодекс РФ вводит уголовную ответственность за правонарушения, связанные с нарушением информационной безопасности.

Статья 137: устанавливает ответственность за нарушение неприкосновенности частной жизни, включая незаконный сбор и распространение информации о частной жизни лица.

Статья 272: вводит ответственность за неправомерный доступ к компьютерной информации, что включает действия, связанные с несанкционированным проникновением в системы и нарушением их работы.

Статья 273: касается разработки, использования и распространения вредоносных программ, что может нарушить нормальную работу информационных систем и повлечь за собой утечку или изменение данных.

Статья 274: регулирует ответственность за нарушение правил эксплуатации информационных систем, которые могут привести к изменению, уничтожению или блокированию информации.

4. Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ № 646 от 5 декабря 2016 года, является стратегическим документом, направленным на защиту национальных интересов в сфере информации.

Основные положения: доктрина описывает угрозы и риски в информационной сфере, а также механизмы защиты, в том числе с использованием программных и программно-аппаратных средств.

Основные направления защиты: доктрина подчеркивает важность защиты государственной информации, персональных данных, а также критической информационной инфраструктуры (кибербезопасность).

Угрозы: к основным угрозам доктрина относит кибератаки, несанкционированное вмешательство в работу информационных систем, утечку конфиденциальной информации, а также влияние иностранных государств в информационной сфере.

Рекомендации: документ устанавливает необходимость использования современных средств криптографической защиты, технологий мониторинга и предотвращения угроз, а также постоянного повышения квалификации специалистов в области информационной безопасности.

Меры защиты: доктрина предписывает использование как организационных, так и технических средств защиты информации, включая программно-аппаратные решения для предотвращения и реагирования на угрозы.

5. Федеральный закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»

Этот закон регулирует вопросы, связанные с охраной государственной тайны, и устанавливает порядок обращения с информацией, важной для безопасности государства.

Определение государственной тайны: информация, которая подлежит защите от несанкционированного доступа и касается военной, экономической, внешнеполитической и других сфер.

Категории секретности: вводятся три уровня секретности — «особой важности», «совершенно секретно» и «секретно», которые указывают на степень защиты данных.

Меры защиты: закон предписывает использование сертифицированных средств защиты, таких как криптографические системы, и строгие меры по предотвращению утечек данных.

Доступ к секретной информации: регулируется порядок получения допуска к государственной тайне, а также процедуры контроля и мониторинга работы с секретными сведениями.

6. Федеральный закон РФ от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»

Этот закон определяет правовые основы работы с информацией и информационными технологиями в России, а также регулирует защиту данных, в том числе с помощью программных и аппаратных средств.

Основные положения: закон устанавливает правила для субъектов информационных отношений, включая обязательства по защите данных и конфиденциальности информации.

Информационные системы: вводятся требования к защите информации в информационных системах, включая необходимость использования программно-аппаратных решений для предотвращения несанкционированного доступа и защиты данных.

Интернет и информационная безопасность: закон регулирует вопросы защиты данных в интернете и требует применения технологий шифрования и контроля доступа.

Требования к обработке данных: организации обязаны использовать программные и аппаратные средства защиты для обеспечения безопасности информации, обрабатываемой в их системах.

7. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»

Закон регулирует обработку, хранение и защиту персональных данных в России и устанавливает требования к обеспечению их безопасности с использованием современных технологий.

Определение персональных данных: это информация, которая позволяет идентифицировать конкретное физическое лицо.

Обработка и хранение данных: закон регулирует порядок сбора, обработки и хранения персональных данных, требуя от операторов принятия мер по защите этих данных.

Технические меры защиты: предписывается использование программно-аппаратных средств, таких как шифрование, системы контроля доступа и мониторинга, для предотвращения несанкционированного доступа к персональным данным.

Обязанности операторов данных: организации, обрабатывающие персональные данные, обязаны внедрять комплексные меры защиты, включая обучение персонала и использование сертифицированных средств защиты информации.

8. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Закон регулирует использование электронной подписи для удостоверения подлинности электронных документов и устанавливает требования к безопасности электронной подписи.

Виды электронной подписи: закон определяет три типа подписи — простую, усиленную неквалифицированную и усиленную квалифицированную. Усиленная квалифицированная подпись требует сертифицированных средств защиты.

Требования по безопасности: усиленная квалифицированная подпись требует использования криптографических средств для создания и хранения ключей подписи.

Юридическая сила: документы, подписанные с помощью усиленной квалифицированной подписи, обладают той же юридической силой, что и бумажные документы с подписью.

9. Федеральный закон от 29.04.2004 № 98-ФЗ «О коммерческой тайне»

Закон регулирует защиту конфиденциальной информации коммерческого характера, которая может иметь экономическую ценность для организации.

Определение коммерческой тайны: это информация, связанная с производственной, научной, технической, экономической и финансовой деятельностью, которая не подлежит разглашению.

Меры защиты: организации обязаны внедрять меры защиты коммерческой тайны, включая программные и аппаратные средства защиты от несанкционированного доступа и утечек.

Контроль доступа: предусматриваются механизмы ограничения доступа к информации, составляющей коммерческую тайну, а также внедрение шифрования и систем мониторинга.

Ответственность: закон устанавливает ответственность за незаконное получение и разглашение информации, составляющей коммерческую тайну, что требует усиленной защиты данных.

10. Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»

Этот указ устанавливает перечень сведений, которые подлежат защите как государственная тайна. Он определяет категории информации, обладающей стратегической важностью для безопасности государства.

Категории сведений: к государственной тайне отнесены данные в области обороны, экономики, внешней политики, науки и техники, разведывательной и контрразведывательной деятельности.

Регулирование доступа: указ предписывает меры по ограничению доступа к таким сведениям, включая использование программных и аппаратных средств защиты для предотвращения несанкционированного доступа к секретной информации.

Требования по защите: организации, работающие с секретными сведениями, обязаны использовать сертифицированные средства защиты, включая криптографические системы и другие технические решения, обеспечивающие безопасность данных.

11. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»

Этот указ устанавливает перечень сведений, которые относятся к конфиденциальной информации, но не составляют государственную тайну. К таким сведениям требуется применять меры защиты, в том числе программно-аппаратные решения.

Конфиденциальная информация: к сведениям конфиденциального характера относятся персональные данные, коммерческая тайна, сведения о профессиональной тайне (врачебной, адвокатской, нотариальной) и другие данные, не подлежащие разглашению без согласия их владельцев.

Защита информации: организации, работающие с конфиденциальными сведениями, обязаны внедрять меры защиты информации, такие как системы шифрования, контроль доступа и мониторинг безопасности.

Ответственность за разглашение: указ устанавливает необходимость предотвращения несанкционированного доступа и утечек конфиденциальной информации, что требует применения современных технических решений для защиты данных.

12. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Это постановление устанавливает требования к защите персональных данных при их обработке в информационных системах и определяет классификацию уровней защищенности таких систем.

Классификация уровней защищенности: информационные системы персональных данных классифицируются по уровням защищенности в зависимости от объема обрабатываемых данных, характера и потенциальных угроз. Чем выше уровень угроз, тем жестче требования к защите.

Технические и организационные меры: постановление предписывает обязательное использование сертифицированных средств защиты информации, включая антивирусные программы, системы шифрования и контроль доступа. Организации должны внедрять административные меры, такие как разработка политики информационной безопасности и регулярное обучение сотрудников.

Аудит безопасности: компании обязаны проводить регулярные проверки своих систем на предмет уязвимостей и соответствия требованиям законодательства.

13. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»

Это постановление регулирует порядок лицензирования деятельности по технической защите конфиденциальной информации, включая требования к организациям, занимающимся такой деятельностью.

Лицензирование: для ведения деятельности по защите конфиденциальной информации необходимо получение лицензии, которая выдается ФСТЭК России. Лицензиаты обязаны выполнять комплекс технических и организационных мер для обеспечения защиты данных.

Требования к соискателям лицензии: организации, желающие получить лицензию, должны соответствовать ряду условий, включая наличие специалистов, квалифицированных в области информационной безопасности, и использование сертифицированных средств защиты.

Контроль и ответственность: организации, имеющие лицензию, подлежат регулярным проверкам со стороны государственных органов на соответствие установленным требованиям.

14. Приказ от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (ФСТЭК)

Этот приказ устанавливает требования к защите информации, не относящейся к государственной тайне, но обрабатываемой в государственных информационных системах.

Требования к защите информации: информационные системы, содержащие конфиденциальные данные, должны соответствовать ряду организационных и технических требований по защите информации, таких как использование систем защиты от несанкционированного доступа и регулярное обновление программного обеспечения.

Меры защиты: вводится обязательное использование антивирусного ПО, системы мониторинга событий безопасности и средства защиты от утечек данных. Также предусматривается использование шифрования для защиты информации при передаче по сетям.

Проверка соответствия: организации, эксплуатирующие государственные информационные системы, обязаны проводить аттестацию систем на соответствие требованиям безопасности.

15. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Этот приказ устанавливает конкретные организационные и технические меры, которые должны быть приняты для защиты персональных данных в информационных системах.

Организационные меры: включают в себя назначение ответственных лиц за защиту персональных данных, разработку внутренней политики безопасности, проведение регулярных инструктажей и обучение персонала.

Технические меры: приказ предписывает использование шифрования для передачи и хранения данных, применение средств аутентификации и контроля доступа, внедрение систем антивирусной защиты и регулярного обновления программного обеспечения.

Мониторинг и аудит: для обеспечения защиты данных организации должны внедрить системы мониторинга безопасности и регулярно проводить аудиты информационных систем на предмет соответствия требованиям законодательства.

16. Руководящие документы ФСТЭК по защите от несанкционированного доступа (НСД)

Руководящие документы ФСТЭК по защите от НСД содержат требования и рекомендации по обеспечению безопасности информации и предотвращению несанкционированного доступа к информационным системам.

Принципы защиты от НСД: применение мер по разграничению доступа, контроль прав доступа к информации, аутентификация пользователей, мониторинг активности и ведение журналов событий безопасности.

Технические средства защиты: использование программных и аппаратных средств защиты, таких как межсетевые экраны, системы обнаружения вторжений и шифрование данных.

Аудит безопасности: регулярное тестирование систем на уязвимости, проведение аудитов на соответствие требованиям по защите от НСД.

17. Руководящие документы ФСТЭК по защите от недекларированных возможностей (НДВ)

Документы по защите от НДВ направлены на предотвращение использования скрытых возможностей в программных средствах, которые могут быть использованы для несанкционированного доступа к информации или компрометации системы.

Определение НДВ: недекларированные возможности — это функции, не заявленные производителем программного обеспечения, которые могут создавать угрозы безопасности.

Методы защиты: включают обязательную сертификацию программного обеспечения, анализ кода на предмет наличия НДВ, а также использование систем мониторинга и контроля за функционированием ПО.

Аттестация программного обеспечения: проводится для подтверждения отсутствия НДВ в программных продуктах, особенно при работе с государственными информационными системами.

18. Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.

Этот документ регламентирует порядок аттестации объектов информатизации в части их соответствия требованиям безопасности информации.

Аттестация объектов: обязательная процедура, направленная на подтверждение соответствия объекта информационной системы установленным нормам безопасности.

Классификация объектов информатизации: объекты разделяются по уровням защищенности в зависимости от типа обрабатываемой информации и потенциальных угроз.

Требования к защите: аттестация требует проведения ряда мер по защите, таких как шифрование данных, внедрение систем контроля доступа, физическая защита оборудования.

19. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)

СТР-К — это документ, содержащий специализированные требования и рекомендации по защите конфиденциальной информации с использованием технических средств.

Принципы защиты: защита информации от несанкционированного доступа, утечек, кражи и других угроз с использованием комплексных средств защиты.

Меры защиты: применение систем криптографической защиты, шифрования данных, контроля доступа, а также физических мер, таких как защита серверных помещений и рабочих мест.

Организационные меры: включают в себя обучение сотрудников, разработку политики информационной безопасности, а также регулярный контроль и аудит защиты информации.

20. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении, разработке, производстве, реализации и эксплуатации шифровальных и криптографических средств защиты (Положение ПКЗ-2005)»

Этот приказ регулирует деятельность по созданию, сертификации, внедрению и эксплуатации шифровальных и криптографических средств защиты информации.

Криптографическая защита: обязательное использование сертифицированных криптографических средств для защиты государственной, конфиденциальной и персональной информации.

Производство и разработка: шифровальные средства могут разрабатываться и производиться только организациями, имеющими соответствующую лицензию от ФСБ России.

Контроль за использованием: эксплуатация криптографических средств подлежит строгому контролю, а организации обязаны вести учет и мониторинг их использования.

**Основные задания**

**Задание 1**

Нормативные методические документы по защите информации

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Устанавливает правовые основы регулирования отношений в области информации, информационных технологий и защиты информации. Определяет требования к использованию программных и программно-аппаратных средств для защиты информации.

2. Федеральный закон № 152-ФЗ «О персональных данных»

Регулирует обработку персональных данных, включая требования по защите данных с использованием технических средств защиты.

3. Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Определяет состав и содержание организационных и технических мер для обеспечения безопасности персональных данных в информационных системах. Включает требования к программным и программно-аппаратным средствам защиты.

4. Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Утверждает требования к обеспечению безопасности информации в автоматизированных системах. Описывает использование программных и программно-аппаратных средств для защиты от несанкционированного доступа и других угроз.

5. Приказ ФСБ России № 149/6/6-622 от 21 февраля 2008 г.

Содержит типовые требования по организации и функционированию криптографических средств для защиты персональных данных. Регулирует использование программных и программно-аппаратных средств шифрования.

6. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»

Устанавливает основные термины и определения в области защиты информации. Включает понятия программных и программно-аппаратных средств защиты.

7. ГОСТ Р 56939-2016 «Информационные технологии. Методы и средства обеспечения безопасности информационных систем»

Определяет методы и средства защиты информации в информационных системах, включая программные и программно-аппаратные решения.

**Задание 2**

Требования и рекомендации по защите информации, изложенные в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации», включают следующие ключевые моменты:

Требования:

* Использование сертифицированных средств защиты:

Программные и программно-аппаратные средства защиты информации должны быть сертифицированы уполномоченными органами (ФСБ, ФСТЭК).

* Защита конфиденциальной информации:

Обязательно использование криптографических средств для защиты конфиденциальной информации.

* Обеспечение целостности, доступности и конфиденциальности:

Информационные системы должны обеспечивать защиту от неправомерного доступа, модификации, уничтожения и других действий, угрожающих безопасности информации.

* Регулярное обновление ПО:

Программное обеспечение должно своевременно обновляться для устранения уязвимостей и поддержания защиты информации.

* Мониторинг и контроль:

Операторы обязаны организовать регулярный контроль и мониторинг состояния системы защиты, а также проводить аудиты безопасности.

Рекомендации:

* Использование встроенных средств защиты:

Программные решения должны содержать механизмы защиты, такие как идентификация, аутентификация, авторизация и шифрование данных.

* Разграничение прав доступа:

Необходимо внедрять системы разграничения прав доступа к информации на основе уровня полномочий пользователей.

* Шифрование данных:

Рекомендуется применять криптографическую защиту при передаче данных через сети связи.

* Тестирование на уязвимости:

Рекомендуется проводить регулярное тестирование программных продуктов для выявления и устранения уязвимостей.

**Задание 3**

Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» содержит требования и рекомендации по защите информации в информационных системах персональных данных (ИСПДн).

Требования:

Сертифицированные средства защиты: Использование сертифицированных ФСТЭК или ФСБ программных и программно-аппаратных средств.

Разграничение доступа: Обеспечение идентификации, аутентификации пользователей и контроля доступа.

Шифрование данных: Использование криптографии для защиты данных при передаче.

Мониторинг и регистрация: Внедрение систем отслеживания событий безопасности.

Контроль целостности: Использование средств для проверки целостности ПО и данных.

Антивирусная защита: Установка и регулярное обновление антивирусных программ.

Защита от утечек: Защита от побочных излучений и наводок.

Рекомендации:

Комплексная защита: Использование программных и аппаратных решений вместе.

Обновление средств защиты: Регулярное обновление ПО.

Аудит безопасности: Регулярное тестирование и аудит защиты.

Минимизация доступа: Предоставление доступа только необходимым пользователям.

**Задание 4**

Типовые требования, утвержденные Центром ФСБ России 21.02.2008 № 149/6/6-622, касаются использования шифровальных (криптографических) средств для защиты персональных данных в информационных системах. Эти требования определяют меры для защиты информации, не содержащей сведений, составляющих государственную тайну.

Требования:

Сертификация: Использование сертифицированных ФСБ криптографических средств.

Шифрование данных: Шифрование персональных данных при передаче и хранении.

Управление ключами: Безопасное хранение и использование ключей.

Ограничение доступа: Доступ к криптосредствам и ключам только авторизованным лицам.

Мониторинг действий: Регистрация всех операций с криптографическими средствами.

Рекомендации:

Комплексная защита: Использование криптографии вместе с другими средствами защиты.

Обновление: Регулярное обновление криптосредств.

Обучение: Подготовка персонала для работы с криптосредствами.

**Вывод**

В ходе работы был проанализирован ряд нормативных актов и методических документов, устанавливающих требования к защите информации программными и программно-аппаратными средствами. Основные положения направлены на обязательное использование сертифицированных средств защиты, шифрование данных и контроль доступа. Соблюдение этих требований обеспечивает надежную защиту информации и минимизирует риски утечек и несанкционированного доступа. Работа подчеркнула важность регулярного обновления мер безопасности в условиях постоянно меняющихся угроз.