УТВЕРЖДЕНО
решением Правления
ТОО «Объединенная химическая компания»
от "23" июля 2010 года
протокол № 16/10

ПОЛИТИКА
информационной безопасности по обеспечению защиты информации в информационных системах ТОО «Объединенная химическая компания»

2010 год

Содержание

Список использованных сокращений и определений

ИС	Информационная система
БД	База данных
ВТСС	Вспомогательные технические средства и системы
ЛВС	Локальная вычислительная сеть
НГМД	Накопитель на гибком магнитном диске
НСД	Несанкционированный доступ
ОБИ	Обеспечение информационной безопасности
ОС	Операционная система
ПЭВМ	Персональная ЭВМ
ПЭМИН	Побочные электромагнитные излучения и наводки
СКЗИ	Средство криптографической защиты информации
СВТ	Средства вычислительной техники
ЭЦП	Электронно-цифровая подпись
СЗКИ	Система защиты конфиденциальной информации
ЭВМ	Электронно-вычислительная машина

ВВЕДЕНИЕ

1.Настоящая Политика информационной безопасности ТОО «Объединенная химическая компания» (далее - Политика) разработана в целях обеспечения защиты информации в информационной системе ТОО «Объединенная химическая компания» (далее - Товарищество).

2.Политика представляет собой систематизированное изложение целей и задач защиты, а также основных принципов и способов достижения требуемого уровня информационной безопасности в Товариществе и описывает основные виды организационно-технических процедур защиты информационных систем, доступа информационных массивов с использованием технических средств, выделенных каналов и сети Интернет.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и основа документа

3.Политика учитывает современное состояние и ближайшие перспективы информационного развития Товарищества, определяет цели, задачи и правовые основы ее создания и эксплуатации, режимы функционирования данной системы, а также содержит анализ угроз безопасности для ресурсов информационной системы (далее - ИС) Товарищества.

4.При разработке Политики использованы основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

5.Положения и требования Политики распространяются на все структурные подразделения Товарищества, в которых осуществляется автоматизированная обработка информации, содержащей сведения, составляющие коммерческую, служебную тайну или персональные данные, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИС Товарищества. Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействие с ИС Товарищества в качестве поставщиков и потребителей (пользователей) информации ИС Товарищества.

6.Политика является методологической основой:

1) формирования и проведения единой политики в области обеспечения безопасности информации в ИС Товарищества;

2) принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление,

отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

3) координации деятельности структурных подразделений Товарищества при проведении работ по созданию, развитию и эксплуатации ИС Товарищества с соблюдением требований обеспечения безопасности информации;

4) разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности информации ИС Товарищества.

7.Политика не регламентирует вопросы организации охраны помещений и обеспечения сохранности и физической целостности компонентов ИС, защиты от стихийных бедствий, сбоев в системе энергоснабжения, а также меры по обеспечению личной безопасности персонала Товарищества. Однако Политика должна быть интегрирована в систему безопасности Товарищества в целом (имущественная, физическая и т.д.), что позволит оптимизировать затраты на построение системы информационной безопасности.

8.Политика базируется на системном подходе, предполагающим проведение исследований, разработку системы защиты информации и процессов ее обработки в ИС с единых методологических позиций с учетом всех факторов, оказывающих влияние на защиту информации, и с позиции комплексного применения различных мер и средств защиты.

9.Основные положения Политики предполагают качественное решение вопросов безопасности информации и не концентрируют внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

2. Объекты защиты

10.Основными объектами информационной безопасности в Товариществе являются:

1) информационные ресурсы с ограниченным доступом, составляющие коммерческую, служебную тайну;

2) иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;

3) процессы обработки информации в ИС - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, разработчики и пользователи системы и ее обслуживающий персонал;

4) информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и

телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты ИС.

2.1. Назначение, цели создания и эксплуатации ИС Товарищества

11.ИС Товарищества предназначена для автоматизации деятельности структурных подразделений и сотрудников Товарищества.

12.Создание и применение ИС Товарищества:

преследует следующие цели:

- повышение качества управления производственными процессами;
- повышение качества контроля за движением материальных и финансовых ресурсов Товарищества;
- повышение оперативности процедур сбора данных Товарищества;
- сокращение финансовых и временных затрат на поддержку внутреннего и внешнего электронного документооборота Товарищества;
- повышение оперативности и обоснованности планирования расходов финансовых ресурсов Товарищества;
- повышение оперативности и обоснованности прогнозирования коммерческой деятельности Товарищества и т.д.

охватывает следующие основные процессы:

- интегрированной обработки информации, формирования и ведения специализированных баз данных;
- взаимодействия с партнерскими организациями;
- информационно-справочного обслуживания структурных подразделений и сотрудников Товарищества;
- анализа и прогнозирования деятельности Товарищества, обоснования принятия управленческих решений.

2.2. Структура, состав и размещение основных элементов ИС, информационные связи с другими объектами

13.ИС Товарищества является распределенной системой, объединяющей автоматизированные системы (подсистемы) подразделений Товарищества в единую корпоративную вычислительную IT сеть.

14.В ИС Товарищества циркулирует информация разных категорий, которая может быть совместно использована различными пользователями из различных подсетей IT сети.

15.В ряде подсистем ИС Товарищества предусмотрено взаимодействие с внешними (государственными и коммерческими, в т.ч. зарубежными) организациями по коммутируемым и выделенным каналам с использованием специальных средств передачи информации.

16.Комплекс технических средств ИС Товарищества включает средства обработки данных (ПЭВМ, серверы БД, почтовые серверы и т.п.), средства обмена данными в ЛВС с возможностью выхода в глобальные сети (кабельная система, мосты, шлюзы, модемы и т.д.), а также средства хранения (в т.ч. архивирования) данных.

17.К основным особенностям функционирования ИС Товарищества, относятся:

1) пространственная распределенность системы;

2) объединение разнообразных технических средств обработки и передачи информации;

3) разнообразие решаемых задач и типов обрабатываемых сведений (данных), сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;

4) объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;

5) непосредственный доступ к вычислительным и информационным ресурсам значительного числа различных категорий пользователей (источников и потребителей информации);

6) наличие каналов взаимодействия с "внешним миром" (источниками и потребителями информации), каналов соединения с платежными и внешними информационными системами;

7) непрерывность функционирования ИС Товарищества;

8) высокая интенсивность информационных потоков в ИС Товарищества;

9) наличие в ИС Товарищества ярко выраженных функциональных подсистем с различными требованиями по уровням защищенности (физически объединенных в единую сеть);

10) разнообразие категорий пользователей системы Товарищества.

18.Общая структурная и функциональная организация ИС Товарищества определяется организационно-штатной структурой Товарищества и задачами, решаемыми его структурными подразделениями с применением средств автоматизации. В самом общем виде, информационная система представляет собой совокупность локальных вычислительных сетей (ЛВС) подразделений Товарищества, объединенных средствами телекоммуникации. Каждая ЛВС в ИС Товарищества объединяет ряд взаимосвязанных и взаимодействующих автоматизированных подсистем (технологических участков), обеспечивающих решение задач отдельными структурными подразделениями Товарищества.

19.Объекты информатизации ИС Товарищества включают:

1) технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);

2) информационные ресурсы, содержащие сведения ограниченного доступа и представленные в виде документов или записей в носителях на магнитной, оптической и другой основе, информационных физических полях, массивах и базах данных;

3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);

4) автоматизированные системы связи и передачи данных (средства телекоммуникации);

5) каналы связи, по которым передается информация (в том числе ограниченного распространения);

6) служебные помещения, в которых циркулирует информация ограниченного распространения;

7) технические средства (звукозаписи, звукоусиления, звуковоспроизведения, изготовления, тиражирования документов, переговорные и телевизионные устройства и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации;

8) технические средства и системы, не обрабатывающие информацию (вспомогательные технические средства и системы - ВТСС), размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения ограниченного распространения.

2.3. Категории информационных ресурсов, подлежащих защите

20.В подсистемах ИС Товарищества циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая, персональные данные работников) и открытые сведения.

В документообороте ИС Товарищества присутствуют:

1) платежные поручения и другие расчетно-денежные документы;

2) отчеты (финансовые, аналитические и др.);

3) сведения о лицевых счетах;

4) обобщенная информация и другие конфиденциальные (ограниченного распространения) документы;

5) производственная и технологическая информация.

21.Защите подлежит вся информация, содержащая:

1) сведения ограниченного распространения, составляющие «коммерческую тайну» и информацию категории «для служебного пользования», доступ к которым ограничен собственником информации (Товариществом) в соответствии с инструкцией и перечнем информации, отнесенной к коммерческой тайне и определенными законом правами;

2) персональные сведения работников Товарищества, доступ к которым ограничен.

2.4. Категории пользователей ИС Товарищества, режимы использования и уровни доступа к информации

22.В Товариществе имеются категории пользователей и обслуживающего персонала, которые должны иметь различные полномочия по доступу к информационным, программным и другим ресурсам ИС:

1) пользователи баз данных (конечные пользователи, сотрудники подразделений Товарищества);

2) ответственные за ведение баз данных (ввод, корректировка, удаление данных в БД);

3) администраторы серверов (файловых серверов, серверов приложений, серверов баз данных) и ЛВС;

4) системные программисты (ответственные за сопровождение общего программного обеспечения) на серверах и рабочих станциях пользователей;

5) разработчики прикладного программного обеспечения;

6) специалисты по обслуживанию технических средств вычислительной техники;

7) сотрудники информационной безопасности (специальных средств защиты) и др.

2.5. Уязвимость основных компонентов ИС Товарищества

23.Наиболее доступными и уязвимыми компонентами ИС Товарищества являются сетевые рабочие станции (АРМ сотрудников подразделений Товарищества), с которых могут быть предприняты попытки несанкционированного доступа к информации (НСД) в сети и попытки совершения несанкционированных действий (непреднамеренных и умышленных). С рабочих станций осуществляется управление процессами обработки информации (в том числе на серверах), запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На мониторы и печатающие устройства рабочих станций выводится информация при работе пользователей, выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Нарушения конфигурации аппаратно-программных средств рабочих станций и неправомерное вмешательство в процессы их функционирования могут приводить к блокированию информации, невозможности своевременного решения важных задач и выходу из строя отдельных АРМ и подсистем.

24.В особой защите нуждаются выделенные файловые серверы, серверы баз данных и серверы приложений. Несанкционированный доступ к защищаемой информации и оказание влияния на работу различных подсистем серверов могут быть осуществлены при использовании недостатков протоколов обмена и средств разграничения удаленного доступа к ресурсам серверов. При этом могут предприниматься попытки как удаленного (со станций сети) так и непосредственного (с консоли сервера) воздействия на работу серверов и их средств защиты.

25.Мосты, шлюзы, маршрутизаторы, коммутаторы и другие сетевые устройства, каналы и средства связи также нуждаются в защите. Они могут быть использованы для реструктуризации и дезорганизации работы сети, перехвата передаваемой информации, анализа трафика и реализации других способов вмешательства в процессы обмена данными.

3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Интересы затрагиваемых при эксплуатации ИС Товарищества субъектов информационных отношений

26.Субъектами правоотношений при использовании ИС Товарищества и обеспечении информационной безопасности являются:

1) Товарищество как собственник информационных ресурсов;

2) структурные подразделения Товарищества, обеспечивающие эксплуатацию системы автоматизированной обработки информации;

3) должностные лица и сотрудники структурных подразделений Товарищества, как пользователи и поставщики информации в ИС Товарищества в соответствии с возложенными на них функциями;

4) юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в ИС Товарищества;

5) другие юридические и физические лица, задействованные в процессе создания и функционирования ИС Товарищества (разработчики компонент ИС, обслуживающий персонал, организации, привлекаемые для оказания услуг в области безопасности информационных технологий и др.).

27.Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

1) конфиденциальности (сохранения в тайне) определенной части информации;

2) достоверности (полноты, точности, адекватности, целостности) информации;

3) защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

4) своевременного доступа (за приемлемое для них время) к необходимой им информации;

5) разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

6) возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

7) защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

3.2. Цели защиты

28.Основной целью, на достижение которой направлены все положения Политики, является защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании ИС Товарищества) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс

функционирования ИС Товарищества или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

29.Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и автоматизированной системы ее обработки:

1) доступности обрабатываемой информации для зарегистрированных пользователей (устойчивого функционирования ИС Товарищества, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);

2) сохранения в тайне (обеспечения конфиденциальности) определенной части информации, хранимой, обрабатываемой ИС Товарищества и передаваемой по каналам связи;

3) целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в ИС Товарищества и передаваемой по каналам связи.

3.3. Основные задачи системы обеспечения информационной безопасности Товарищества

30.Для достижения основной цели защиты и обеспечения указанных свойств информации и автоматизированной системы ее обработки необходимо обеспечить эффективное решение следующих задач:

1) целостности и аутентичности (подтверждение авторства) информации, обеспечивая защиту от вмешательства в процесс функционирования ИС Товарищества посторонних лиц (возможность использования автоматизированной системы и доступ к ее ресурсам должны иметь только зарегистрированные в установленном порядке пользователи - сотрудники структурных подразделений Товарищества);

2) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС Товарищества (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИС Товарищества для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

к информации, циркулирующей в ИС Товарищества;

средствам вычислительной техники ИС Товарищества;

аппаратным, программным и криптографическим средствам защиты, используемым в ИС Товарищества;

3) регистрацию действий пользователей при использовании защищаемых ресурсов ИС Товарищества в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов сотрудниками, в функции которых входит данная обязанность;

4) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

5) защиту от несанкционированной модификации и контроль целостности используемых в ИС Товарищества программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

6) защиту информации ограниченного распространения от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

7) защиту информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

8) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

9) обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

10) своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

11) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

3.4.Основные пути достижения целей защиты (решения задач системы защиты)

31.Поставленные основные цели и задачи защиты информации достигаются:

1) строгим учетом всех подлежащих защите ресурсов ИС (информации, задач, каналов связи, серверов, автоматизированных рабочих мест – АРМ);

2) регламентацией процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников структурных подразделений Товарищества, использующих ИС Товарищества, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств ИС Товарищества, на основе утвержденных руководством Товарищества организационно-распорядительных документов по вопросам обеспечения безопасности информации;

3) полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Товарищества по вопросам обеспечения безопасности информации;

4) назначением и подготовкой сотрудников Товарищества, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

5) наделением каждого сотрудника Товарищества (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам ИС Товарищества;

6) четким знанием и строгим соблюдением всеми сотрудниками Товарищества, использующими и обслуживающими аппаратные и программные средства ИС Товарищества, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

7) персональной ответственностью за свои действия каждого сотрудника Товарищества, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам ИС Товарищества;

8) реализацией технологических процессов обработки информации с использованием комплексов организационно - технических мер защиты программного обеспечения, технических средств и данных;

9) принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов ИС Товарищества;

10) применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

11) разграничением потоков информации, предусматривающим предупреждение попадания информации более высокого уровня конфиденциальности на носители и в файлы с более низким уровнем конфиденциальности, а также запрещением передачи информации ограниченного распространения по незащищенным каналам связи;

12) эффективным контролем за соблюдением сотрудниками структурных подразделений Товарищества - пользователями ИС Товарищества требований по обеспечению безопасности информации;

13) юридической защитой интересов Товарищества при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;

14) проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в ИС Товарищества.

4. ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИС ТОВАРИЩЕСТВА

4.1 Угрозы безопасности информации и их источники

32.Наиболее опасными (значимыми) угрозами безопасности информации ИС Товарищества (способами нанесения ущерба субъектам информационных отношений) являются:

1) нарушение конфиденциальности (разглашение, утечка) сведений ограниченного распространения;

2) нарушение работоспособности (дезорганизация работы) ИС Товарищества, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

3) нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов ИС Товарищества, а также фальсификация (подделка) документов.

33.Основными источниками угроз безопасности информации ИС Товарищества являются:

1) непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия сотрудников (в том числе администраторов средств защиты) структурных подразделений Товарищества при эксплуатации ИС Товарищества, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих станций (АРМ), подсистем или ИС Товарищества в целом;

2) преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия сотрудников структурных подразделений Товарищества, допущенных к работе с ИС Товарищества, а также сотрудников подразделений Товарищества, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения безопасности информации;

3) воздействия из других логических и физических сегментов ИС Товарищества со стороны сотрудников других подразделений Товарищества, в том числе программистов - разработчиков прикладных задач, а также удаленное несанкционированное вмешательство посторонних лиц из телекоммуникационной сети Товарищества и внешних сетей общего назначения (прежде всего Internet) через легальные и несанкционированные каналы подключения сети Товарищества к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам ИС Товарищества;

4) деятельность международных и отечественных преступных групп и формирований, политических и экономических структур, а также отдельных

лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и ее отдельных компонент;

5) деятельность иностранных специальных служб, направленная против интересов Товарищества;

6) ошибки, допущенные при проектировании ИС Товарищества и ее системы защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты) ИС Товарищества;

7) аварии, стихийные бедствия и т.п.

4.2. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации в ИС Товарищества

34.Пользователи, операторы, системные администраторы и сотрудники Товарищества, обслуживающие ИС, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

35.Основные пути реализации непреднамеренных искусственных (субъективных) угроз ИС Товарищества (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба приведены в Таблице 4.1.

Таблица 4.1.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз ИС Товарищества	**Меры по нейтрализации угроз и снижению возможного наносимого ущерба**
Действия сотрудников Товарищества, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств; отключению оборудования или изменение режимов работы устройств и про грамм; разрушению информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.)	1.Организационные меры (регламентация действий, введение запретов). 2.Применение физических средств, препятствующих неумышленному совершению нарушения. 3.Применение технических (аппаратно-программных) средств разграничения доступа к ресурсам. 4.Резервирование критичных ресурсов.
Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания), или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)	1. Организационные меры (удаление всех потенциально опасных про грамм с дисков ПЭВМ АРМ). 2.Применение технических (аппаратно-программных) средств разграничения доступа к технологическим и инструментальным программам на дисках ПЭВМ АРМ.

Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)	1.Организационные меры (введение запретов). 2.Применение технических (аппаратно-программных) средств, препятствующих несанкционированному внедрению и использованию неучтенных программ.
Непреднамеренное заражение компьютера вирусами	1.Организационные меры (регламентация действий, введение запретов). 2.Технологические меры (применение специальных программ обнаружения и уничтожения вирусов). 3.Применение аппаратно программных средств, препятствующих заражению компьютеров компьютерными вирусами.
Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т.п.)	1.Организационные меры (регламентация действий, введение запретов, усиление ответственности) . 2.Применение физических средств обеспечения сохранности указанных реквизитов.
Игнорирование организационных ограничений (установленных правил) при работе в системе	1.Организационные меры (усиление ответственности и контроля). 2.Использование дополнительных физических и технических средств защиты.
Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом подразделения безопасности	Организационные меры (обучение персонала, усиление ответственности и контроля).
Ввод ошибочных данных	1.Организационные меры (усиление ответственности и контроля). 2.Технологические меры контроля за ошибками операторов ввода данных.

4.3. Умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала

36.Возможные пути умышленной дезорганизации работы, вывода ИС Товарищества из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания

отомстить и т.п.) и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба приведены в Таблице 4.2.

Таблица 4.2.

Основные возможные пути умышленной дезорганизации работы, вывода ИС Товарищества из строя, проникновения в систему и НСД к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.)	**Меры по нейтрализации угроз и снижению возможного наносимого ущерба**
Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов корпоративной сети (устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.)	1.Организационные меры (регламентация действий, введение запретов). 2.Применение физических средств, препятствующих умышленному совершению нарушения. 3.Резервирование критичных ресурсов. 4.Обеспечение личной безопасности сотрудников.
Внедрение агентов в число персонала системы (в том числе возможно и в административную группу, отвечающую за безопасность), вербовка (путем подкупа, шантажа, угроз и т.п.) пользователей, имеющих определенные полномочия по доступу к защищаемым ресурсам.	Организационные меры (подбор, расстановка и работа с кадрами, усиление контроля и ответственности). Автоматическая регистрация действий персонала.
Хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.)	Организационные меры (организация хранения и использования носителей с защищаемой информацией).
Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.	1.Организационные меры (организация хранения и использования носителей с защищаемой информацией). 2.Применение технических средств разграничения доступа к защищаемым ресурсам и автоматической регистрации получения твердых копий документа.
Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем	1.Организационные меры (регламентация действий, введение запретов, работа с кадрами). 2.Применение технических средств,

имитации интерфейса системы программными закладками и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»).	препятствующих внедрению программ перехвата паролей, ключей и других реквизитов.
Несанкционированное использование АРМ пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.	1.Организационные меры (строгая регламентация доступа в помещения и допуска к работам на данных АРМ). 2.Применение физических и технических средств разграничения доступа.
Несанкционированная модификация программного обеспечения – внедрение программных «закладок» и «вирусов» («троянских коней» и «жучков»), т.е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования системы.	1.Организационные меры (строгая регламентация допуска к работам). 2.Применение физических и технических средств разграничения доступа и препятствующих несанкционированной модификации аппаратно – программной конфигурации АРМ. 3.Применение средств контроля целостности программ.
Перехват данных, передаваемых по каналам связи, и их анализ с целью получения конфиденциальной информации и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему.	1.Физическая защита каналов связи. 2.Применение средств криптографической защиты передаваемой информации.
Вмешательство в процесс функционирования ИС сетей общего пользования с целью несанкционированной модификации данных, доступа к конфиденциальной информации, дезорганизации работы подсистем и т.п.	1.Организационные меры (регламентация подключения и работы в сетях общего пользования). 2.Применение специальных технических средств защиты (межсетевых экранов, средств контроля защищенности и обнаружения атак на ресурсы системы и т.п.).

4.4. Утечка информации по техническим каналам

37.При проведении мероприятий и эксплуатации технических средств ИС возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

1) побочные электромагнитные излучения информативного сигнала от технических средств ИС Товарищества и линий передачи информации;

2) наводки информативного сигнала, обрабатываемого ИС Товарищества, на провода и линии, выходящие за пределы контролируемой зоны Товарищества, в т.ч. на цепи заземления и электропитания;

3) изменения тока потребления, обусловленные обрабатываемыми ИС Товарищества информативными сигналами;

4) радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав ИС Товарищества, или при наличии паразитной генерации в узлах (элементах) ИС Товарищества;

5) электрические сигналы или радиоизлучения, обусловленные воздействием на ИС Товарищества высокочастотных сигналов, создаваемых с помощью специальной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом (облучение, «навязывание»);

6) радиоизлучения или электрические сигналы от внедренных в ИС Товарищества и выделенные помещения специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом;

7) радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

8) акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации (телеграф, телетайп, принтер, пишущая машинка и т.п.);

9) электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

10) вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;

11) просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;

12) воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства («закладки»).

38.Перехват информации ограниченного распространения или воздействие на нее с использованием технических средств может вестись

непосредственно из зданий, расположенных в непосредственной близости от объектов информатизации, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими подразделений Товарищества, а также с помощью скрытно устанавливаемой в районах важнейших объектов и на их территориях автономной автоматической аппаратуры.

39.В качестве специальной аппаратуры или воздействия на информацию и технические средства могут использоваться:

1) космические средства для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций, и приема сигнала от автономных автоматических средств и электронных устройств перехвата информации («закладок»);

2) стационарные средства, размещаемые в зданиях;

3) портативные возимые и носимые средства, размещаемые в зданиях, в транспортных средствах, а также носимые лицами, имеющими намерения нанести ущерб Товариществу;

4) автономные автоматические средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

40.Стационарные средства обладают наибольшими энергетическими, техническими и функциональными возможностями. В то же время они, как правило, удалены от объектов защиты и не имеют возможности подключения к линиям, коммуникациям и сооружениям. Портативные средства могут использоваться непосредственно на объектах защиты или поблизости от них и могут подключаться к линиям и коммуникациям, выходящим за пределы контролируемой территории.

41.Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна вследствие:

1) непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;

2) случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;

3) просмотра информации с экранов дисплеев и других средств ее отображения.

4.5. Неформальная модель возможных нарушителей

42.Нарушитель - это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или

удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

43.Система защиты ИС Товарищества должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

1) "Неопытный (невнимательный) пользователь" - сотрудник Товарищества (или подразделения другого ведомства, зарегистрированный как пользователь системы), который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам ИС с превышением своих полномочий, ввода некорректных данных и т.п., действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

2) "Любитель" - сотрудник Товарищества (или подразделения другого ведомства, зарегистрированный как пользователь системы), пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из «спортивного интереса». Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

3) "Мошенник" - сотрудник Товарищества (или подразделения другого ведомства, зарегистрированный как пользователь системы), который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого сотрудника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

4) "Внешний нарушитель (злоумышленник)" - постороннее лицо или сотрудник Товарищества (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения безопасности информации, методов и средств взлома систем защиты, характерных для сетей общего пользования

(в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети ИС Товарищества.

5) "Внутренний злоумышленник" - сотрудник подразделения Товарищества, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками Товарищества. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне - из сетей общего пользования.

44.Внутренним нарушителем может быть лицо из следующих категорий персонала Товарищества:

1) зарегистрированные конечные пользователи ИС Товарищества (сотрудники подразделений Товарищества);

2) сотрудники подразделений Товарищества, не допущенные к работе с ИС Товарищества;

3) персонал, обслуживающий технические средства ИС Товарищества (инженеры, техники);

4) сотрудники подразделений разработки и сопровождения ПО (прикладные и системные программисты);

5) технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС Товарищества);

6) руководители структурных подразделений Товарищества,

45.Категории лиц, которые могут быть внешними нарушителями:

1) уволенные сотрудники Товарищества;

2) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);

3) посетители (приглашенные представители организаций, граждане) представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.;

4) члены преступных организаций, сотрудники специальных служб или лица, действующие по их заданию;

5) лица, случайно или умышленно проникшие в сети ИС Товарищества из внешних (по отношению к Товариществу) сетей телекоммуникации (хакеры).

46.Пользователи и обслуживающий персонал из числа сотрудников Товарищества имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

47.Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в ИС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками Товарищества и криминальными структурами.

48.Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Криминальные структуры могут использовать эти организации для временного устройства на работу своих членов с целью доступа к защищаемой информации в ИС Товарищества.

49.Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

1) работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей - сотрудников Товарищества по преодолению системы защиты;

2) нарушитель скрывает свои несанкционированные действия от других сотрудников Товарищества;

3) несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

4) в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

5. ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕХНИЧЕСКОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИС ТОВАРИЩЕСТВА

5.1. Техническая политика в области обеспечения безопасности информации

50.Техническая политика в области обеспечения безопасности информации должна предусматривать системное согласование между собой

и комплексное применение технических (аппаратных, программных) средств и организационных мероприятий при их оптимальном соотношении.

51.Основными направлениями реализации технической политики обеспечения безопасности информации ИС Товарищества являются:

1) обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий (от НСД);

2) обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

52.Система обеспечения безопасности информации ИС Товарищества должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании импортных технических и программных средств.

53.В рамках указанных направлений технической политики обеспечения безопасности информации осуществляются:

1) реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации конфиденциального характера;

2) реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

3) ограничение доступа исполнителей и посторонних лиц в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация конфиденциального характера, непосредственно к самим средствам информатизации и коммуникациям;

4) разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защита информации в подсистемах различного уровня и назначения, входящих в ИС Товарищества;

5) учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

6) предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок;

7) криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

8) надежное хранение традиционных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;

9) необходимое резервирование технических средств и дублирование массивов и носителей информации;

10) снижение уровня и информативности ПЭМИН, создаваемых различными элементами автоматизированных подсистем;

11) обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;

12) электрическая развязка цепей питания, заземления и других цепей объектов информатизации, выходящих за пределы контролируемой зоны;

13) активное зашумление в различных диапазонах;

14) противодействие оптическим и лазерным средствам наблюдения;

15) обеспечение противопожарной безопасности.

5.2. Формирование режима безопасности информации

54.С учетом выявленных угроз безопасности информации ИС Товарищества режим защиты должен формироваться как совокупность способов и мер защиты циркулирующей в автоматизированной системе информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

55.Комплекс мер по формированию режима безопасности информации включает:

1) установление в Товариществе организационно-правового режима безопасности информации (нормативные документы, работа с персоналом, делопроизводство);

2) выполнение организационно-технических мероприятий по защите информации ограниченного распространения от утечки по техническим каналам;

3) организационные и программно-технические мероприятия по предупреждению несанкционированных действий (доступа) к информационным ресурсам ИС Товарищества;

4) комплекс мероприятий по контролю функционирования средств и систем защиты информационных ресурсов ограниченного распространения после случайных или преднамеренных воздействий;

5) комплекс оперативных мероприятий подразделений безопасности по предотвращению (выявлению) проникновения в Товарищество информаторов, связанных с преступными группировками.

5.3. Оснащение техническими средствами хранения и обработки информации

56.Организация хранения конфиденциальных документов и машинных носителей информации, а также оборудование режимных помещений осуществляется в соответствии с установленными в Товариществе требованиями.

57.В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции, утверждаемой Председателем Правления Товарищества после согласования с заинтересованными структурными подразделениями.

58.На случай пожара, аварии или стихийного бедствия разрабатывается инструкция, утверждаемая Председателем Правления Товарищества, в которой предусматривается порядок вызова ответственных сотрудников, вскрытия охраняемых помещений, очередность и порядок спасения конфиденциальных документов и изделий и дальнейшего их хранения. Инструкция должна находиться в соответствующих подразделениях.

59.Режимный объект обеспечивается средствами уничтожения документов.

60.В случае применения для обработки конфиденциальной информации средств вычислительной техники, внедряется система защиты конфиденциальной информации (СЗКИ), которая направлена на обеспечение сохранности информации во время разработки, монтажа, эксплуатации, ремонта и списания СВТ путем предотвращения случаев несанкционированного доступа к информации, ее утечки за счет побочных электромагнитных излучений и наводок и разрушения.

61.Обработка конфиденциальной информации на СВТ разрешается только после завершения работ по внедрению СЗКИ, проверки ее функционирования и аттестации. На период до внедрения и аттестации СЗКИ конфиденциальная информация может обрабатывается на СВТ при полном отключении его от любых средств обмена данными в ЛВС с возможностью выхода в глобальные сети (кабельная система, мосты, шлюзы, модемы и т.д). Электронные носители конфиденциальной информации должны храниться в сейфах и запираемых на ключ металлических шкафах.

62.Работы по обеспечению безопасности информации, обрабатываемой с помощью ИС Товарищества, можно условно разделить на следующие группы:

1) обеспечение физической безопасности компонентов ИС Товарищества (специально внедренные закладные устройства, побочные электромагнитные излучения и наводки, повреждения, сбои питания, кражи и т.п.);

2) обеспечение логической безопасности ИС Товарищества (защита от несанкционированного доступа, от ошибок в действиях пользователей и программ и т.д.);

3) обеспечение социальной безопасности ИС Товарищества (разработка организационных документов, соответствующих законодательным нормам, регулирующих применение компьютерных технологий, порядок расследования и наказания за допущенные нарушения, контроль и предотвращение неправильного использования информации в случае, когда она хранится или обрабатывается с помощью компьютерных систем).

6. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

63. Основные принципы построения системы комплексной защиты информации:

1) законность;
2) системность;
3) комплексность;
4) непрерывность;
5) своевременность;
6) преемственность и непрерывность совершенствования;
7) разумная достаточность;
8) персональная ответственность;
9) минимизация полномочий;
10) взаимодействие и сотрудничество;
11) гибкость системы защиты;
12) открытость алгоритмов и механизмов защиты;
13) простота применения средств защиты;
14) научная обоснованность и техническая реализуемость;
15) специализация и профессионализм;
16) обязательность контроля.

Законность

64.Предполагает осуществление защитных мероприятий и разработку системы безопасности информации ИС Товарищества в соответствии с действующим законодательством Республики Казахстан в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

65.Пользователи и обслуживающий персонал ИС Товарищества должны иметь представление об ответственности за нарушения в области систем автоматизированной обработки информации.

Системность

66.Системный подход к построению системы защиты информации в ИС Товарищества предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации ИС Товарищества.

67.При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность

68.Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты

69.Защита информации - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Товарищества, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

70.Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Своевременность

71.Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС в целом и ее системы защиты информации, в частности.

72.Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и совершенствование

73.Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат)

74.Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы ИС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

75.Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Персональная ответственность

76.Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае

любого нарушения круг виновников был четко известен или сведен к минимуму.

Принцип минимизации полномочий

77.Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество

78.Предполагает создание благоприятной атмосферы в коллективах структурных подразделений Товарищества. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

Гибкость системы защиты

79.Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев ИС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

80.Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

81.Механизмы защиты должны быть интуитивно понятны и просты в использовании.

82.Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Научная обоснованность и техническая реализуемость

83.Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки

зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

Специализация и профессионализм

84.Предполагает привлечение к разработке средств и реализации мер защиты информации профессионально подготовленных специалистов Товарищества (работников структурных подразделений, имеющих отношение к организации и контролю систем безопасности).

Обязательность контроля

85.Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

86.Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

7. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

7.1. Меры обеспечения безопасности

87.Все меры обеспечения безопасности компьютерных систем подразделяются на:

1) правовые (законодательные);
2) морально-этические;
3) организационные (административные);
4) физические;
5) технические (аппаратурные и программные).

7.1.1. Меры защиты информационных ресурсов

88.К правовым мерам защиты относятся нормативные правовые акты Республики Казахстан, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

7.1.2. Морально-этические меры защиты

89.К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или Товариществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

7.1.3. Организационные (административные) меры защиты

90.Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Формирование политики безопасности

91.Главная цель административных мер, предпринимаемых на высшем управленческом уровне - внедрить данную политику в области обеспечения безопасности информации (отражающую подходы к защите информации), обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

92.С практической точки зрения политику в области обеспечения безопасности информации в ИС Товарищества целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Товарищества в целом. Примером таких решений могут быть:

1) принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности информации, определение ответственных за ее реализацию;

2) формулирование целей, постановка задач, определение направлений деятельности в области безопасности информации;

3) принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Товарищества в целом;

4) обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

93.Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить

какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИС.

94.Политика нижнего уровня определяет процедуры и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

1) какова область применения политики безопасности информации;

2) каковы роли и обязанности ответственных сотрудников, отвечающих за проведение политики безопасности информации;

3) кто имеет права доступа к информации ограниченного распространения;

4) кто и при каких условиях может читать и модифицировать информацию и т.д.

95.Политика нижнего уровня должна:

1) предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении конфиденциальных информационных ресурсов;

2) определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации ограниченного распространения;

3) выбирать программно-математические и технические (аппаратные) средства криптозащиты, противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

<u>Регламентация доступа в помещения ИС Товарищества</u>

96.Эксплуатация защищенных АРМ и серверов ИС Товарищества должна осуществляться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (АРМ, документов, реквизитов доступа и т.п.). Размещение и установка технических средств ПЭВМ таких как АРМ должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения. Уборка помещений с установленными в них ПЭВМ должна производиться в присутствии ответственного, за которым закреплены данные технические средства, или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

97.В помещениях во время обработки и отображения на ПЭВМ информации ограниченного распространения должен присутствовать только персонал, допущенный к работе с данной информацией. Запрещается прием

посетителей и нахождение посторонних лиц в помещениях, когда осуществляется обработка защищаемой информации.

98.Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами.

99.В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции, утверждаемой Председателем Товарищества.

100.Помещения должны быть обеспечены средствами уничтожения документов.

101.В случае применения для обработки информации средств вычислительной техники, пропускной и внутриобъектовый режим объекта СВТ должен удовлетворять требованиям, предъявляемым к режимным объектам.

<u>Регламентация допуска сотрудников к использованию ресурсов ИС Товарищества</u>

102.В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях; система разграничения доступа, которая предполагает определение для всех пользователей автоматизированной информационной системы информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

103.Допуск сотрудников подразделений Товарищества к работе с автоматизированной системой и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем ИС должны производиться в установленном порядке. Основными пользователями информации в ИС Товарищества являются сотрудники структурных подразделений Товарищества. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

1) открытая, конфиденциальная информация размещаются по возможности на различных серверах, это упрощает обеспечение защиты;

2) каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями;

3) начальник имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;

4) наиболее ответственные технологические операции должны производиться по правилу "в две руки" - правильность введенной

информации подтверждается другим ответственным сотрудником, не имеющим права ввода информации.

104.Все сотрудники Товарищества, допущенные к работе (пользователи) и обслуживающий персонал ИС Товарищества, должны нести персональную ответственность за нарушения установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник должен подписывать обязательство о соблюдении правил работы с защищаемой информацией в ИС Товарищества.

105.Обработка защищаемой информации в подсистемах ИС Товарищества должна производиться в соответствии с утвержденными технологическими инструкциями (техническими порядками) для данных подсистем.

106.Для пользователей защищенных АРМ (то есть АРМ, на которых обрабатывается защищаемая информация или решаются подлежащие защите задачи и на которых установлены соответствующие средства защиты) должны быть разработаны необходимые технологические инструкции, включающие требования по обеспечению безопасности информации.

Регламентация процессов ведения баз данных и осуществления модификации информационных ресурсов

107.Все операции по ведению баз данных Товарищества и допуск сотрудников подразделений Товарищества к работе с этими базами данных должны быть строго регламентированы и производиться в соответствии с утвержденными технологическими инструкциями. Распределение имен, генерация паролей, сопровождение правил разграничения доступа к базам данных возлагается на специальных пользователей - администраторов конкретных баз данных. При этом могут использоваться, как только штатные, так и дополнительные средства защиты СУБД и операционных систем.

Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИС Товарищества

108.Все аппаратные и программные ресурсы ИС Товарищества должны быть в установленном порядке категорированы (для каждого ресурса должен быть определен требуемый уровень защищенности). Подлежащие защите ресурсы системы (задачи, программы, АРМ) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

109.Аппаратно-программная конфигурация автоматизированных рабочих мест, на которых обрабатывается защищаемая информация (с которых возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей данного АРМ функциональных обязанностей. Все неиспользуемые в работе (лишние) устройства ввода-вывода информации (COM, LPT порты, дисководы НГМД, CD с других носителей информации) на таких АРМ должны быть отключены (удалены),

не нужные для работы программные средства и данные с дисков АРМ также должны быть удалены.

110.Для упрощения сопровождения, обслуживания и организации защиты АРМ должны оснащаться программными средствами и конфигурироваться унифицировано.

111.Ввод в эксплуатацию новых АРМ и все изменения в конфигурации технических и программных средств существующих АРМ в ИС Товарищества должны осуществляться только в установленном порядке.

112.Все программное обеспечение (разработанное специалистами Товарищества, полученное централизованно или приобретенной у фирм - производителей и поставщиков) должно в установленном порядке проходить испытания и причисляться к списку разрешенного к использованию ПО Товарищества. В подсистемах ИС должно устанавливаться и использоваться только разрешенное к использованию ПО Товарищества. Использование не учтенного ПО в ИС, должно быть запрещено.

113.Разработка ПО задач (комплексов задач), проведение испытаний разработанного и приобретенного ПО, передача ПО в эксплуатацию должна осуществляться в соответствии с установленным порядком разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию.

Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов ИС Товарищества

114.На всех АРМ, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие категории данных АРМ).

115.Узлы и блоки оборудования СВТ, к которым доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к их монтажным схемам должны закрываться и опечатываться (пломбироваться) сотрудниками Товарищества, ответственными за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки. О вскрытии (опечатывании) блоков ПЭВМ делается запись в соответствующем журнале.

116.Повседневный контроль за целостностью и соответствием печатей (пломб) на системных блоках ПЭВМ должен осуществляться пользователями АРМ и ответственными за безопасность информации подразделений работниками Товарищества. Периодический контроль - сотрудниками Товарищества, ответственными за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки.

Кадровая работа (подбор и подготовка персонала. обучение пользователей)

117.До начала этапа эксплуатации автоматизированной системы ее пользователи, а также необходимый руководящий и обслуживающий персонал должны быть ознакомлены с перечнем сведений, относящихся к

коммерческой, служебной тайне и конфиденциальным сведениям в Товариществе, в части их касающейся, и своим уровнем полномочий, а также организационно - распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации ограниченного распространения.

118.Защита информации по всем перечисленным направлениям возможна только после выработки у пользователей определенной дисциплины, т.е. норм, обязательных для исполнения всеми, кто работает с ИС Товарищества. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу ИС Товарищества, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей.

119.Все сотрудники Товарищества, использующие при работе конкретные подсистемы ИС Товарищества, должны быть ознакомлены с организационно-распорядительными документами по защите ИС Товарищества в части, их касающейся, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации при использовании ИС. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

Подразделения обеспечивающие защиту информации

120.Для непосредственной организации (построения) и эффективного функционирования системы защиты информации в Товариществе должно быть организованно подразделение с функциями по защите информации или назначены сотрудники Товарищества для выполнения данной функции.

121.Данное подразделение для выполнения мероприятий по защите информации должна представлять собой сотрудников, предназначенных для организации квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования во всех подразделениях Товарищества.

122.На этих сотрудников целесообразно возложить решение следующих основных задач:

1) проведение в жизнь политики обеспечения безопасности информации, определение требований к системе защиты информации;
2) организация мероприятий и координация работ всех подразделений Товарищества по комплексной защите информации;
3) контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

123.Основные функции сотрудников структурного подразделения по обеспечению защиты информации в информационных системах заключаются в следующем:

1) формирование требований к системе защиты в процессе создания (развития) ИС Товарищества;

2) участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;

3) планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования ИС;

4) распределение между пользователями необходимых реквизитов защиты;

5) наблюдение за функционированием системы защиты и ее элементов;

6) организация проверок надежности функционирования системы защиты;

7) обучение пользователей и персонала ИС правилам безопасной обработки информации;

8) регламентация действий и контроль за администраторами баз данных, серверов и сетевых устройств (за сотрудниками, обеспечивающими правильность применения имеющихся в составе ОС, СУБД и т.п. средств разграничения доступа и других средств защиты информации);

9) взаимодействие с сотрудниками ответственными за соблюдение информационной безопасности в подразделениях Товарищества;

10) контроль за соблюдением пользователями и персоналом правил обращения с защищаемой информацией автоматизированной обработки;

11) принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

124.Статус сотрудников структурного подразделения по обеспечению защиты информации в информационных системах определяется следующим образом:

1) численность сотрудников должна быть достаточной для выполнения всех перечисленных выше функций;

2) сотрудники службы должны иметь право доступа во все помещения Товарищества, где установлена аппаратура ИС Товарищества и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;

3) руководителю данного подразделения должно быть предоставлено право запрещать включение в число действующих новые элементы ИС Товарищества, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз безопасности информации;

4) данное подразделение должно быть обеспечено всеми условиями, необходимыми для выполнения своих функций.

125.Для решения задач по обеспечению защиты информации в информационных системах сотрудники должны иметь следующие права:

1) определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность сотрудников подразделений Товарищества;

2) получать информацию от сотрудников подразделений Товарищества по вопросам применения информационных технологий и эксплуатации ИС;

3) участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке комплексов задач (задач);

4) участвовать в испытаниях разработанных комплексов задач (задач) по вопросам оценки качества реализации требований по обеспечению безопасности информации;

5) контролировать деятельность сотрудников подразделений Товарищества по вопросам ОБИ.

126.В состав подразделения по обеспечению защиты информации в информационных системах должны входить следующие специалисты:

1) ответственные за администрирование средств защиты от НСД (выбор, установка, настройка, снятие средств защиты, просмотр журналов регистрации событий, оперативный контроль за работой пользователей и реагирование на события НСД и т.п.);

2) ответственные за администрирование криптографических средств защиты (установка, настройка, снятие СКЗИ, генерация и распределение ключей и т.д.);

3) ответственные за решение вопросов защиты информации в разрабатываемых программистами и внедряемых прикладных программах (участие в разработке технических заданий по вопросам защиты информации, выбор средств и методов защиты, участие в испытаниях новых прикладных программ с целью проверки выполнения требований по защите информации и т.д.);

4) специалисты по защите от утечки информации по техническим каналам.

Ответственность за нарушения установленного порядка использования ИС Товарищества. Расследование нарушений.

127.Любое грубое нарушение порядка и правил работы в ИС сотрудниками структурных подразделений Товарищества должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Товарищества.

128.Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

1) индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора, на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

2) проверка подлинности пользователей (аутентификация) на основе паролей, ключей на различной физической основе, биометрических характеристик личности и т.п.;

3) регистрация (протоколирование) работы ресурсам информационных систем с идентификаторов запрашивающего и взаимодействия и его результата;

4) реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

7.2. Физические средства защиты

129.Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

7.2.1. Разграничение доступа на территорию и в помещения

130.Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны специальных технических средств.

131.Более современными, надежными системами физической защиты, дающими широкие возможности регистрации и контроля за доступом исполнителей и посторонних лиц в помещения, в которых проводятся работы и переговоры секретного (конфиденциального) характера, обрабатывается и хранится такая информация, являются технические системы, основанные на таких методах идентификации и аутентификации персонала как магнитные и электронные карты с личными данными, биометрические характеристики личности, реализуемые в виде автоматизированных систем контроля за доступом в указанные помещения. Подобные автоматизированные системы могут быть реализованы на центральной ПЭВМ, собирающей информацию с большого количества терминалов, контролирующих доступ в помещения, к объектам и отдельным средствам информатизации.

132.Для обеспечения физической безопасности компонентов ИС Товарищества необходимо осуществлять ряд организационных и технических мероприятий, включающих (кроме выполнения рекомендаций по инженерной и технической защите зданий и помещений):

1) проверку поступающего оборудования ИС Товарищества, предназначенного для обработки закрытой (конфиденциальной) информации, на:

наличие специально внедренных закладных устройств;

побочные электромагнитные излучения и наводки;

2) введение дополнительных ограничений по доступу в помещения (компьютерный зал, серверная и т.д.), предназначенные для хранения и обработки закрытой информации;

3) оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

7.3. Технические (программно-аппаратные) средства защиты

133.Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИС Товарищества и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

134.С учетом всех требований и принципов обеспечения безопасности информации в ИС по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

1) средства аутентификации потребителей (пользователей) и элементов ИС Товарищества (терминалов, задач, элементов баз данных и т.п.), соответствующих степени конфиденциальности информации и обрабатываемых данных;

2) средства разграничения доступа к данным;

3) средства криптографического закрытия информации в линиях передачи данных и в базах данных;

4) средства регистрации обращения и контроля за использованием защищаемой информации;

5) средства реагирования на обнаруженный НСД;

6) средства снижения уровня и информативности ПЭМИН, создаваемых различными элементами ИС;

7) средства снижения уровня акустических излучений, сопровождающих функционирование элементов ИС;

8) средства маскировки от оптических средств наблюдения;

9) средства электрической развязки как элементов ИС, так и конструктивных элементов помещений, в которых размещается ИС (включая водопроводную и канализационную систему);

10) средства активного зашумления в радио и акустическом диапазонах.

135.На технические средства защиты от НСД возлагается решение следующих основных задач:

1) идентификация и аутентификации пользователей при помощи имен и/или специальных аппаратных средств;

2) регламентация доступа пользователей к физическим устройствам компьютера (дискам, портам ввода-вывода);

3) избирательное (дискреционное) управление доступом к логическим дискам, каталогам и файлам;

4) полномочное (мандатное) разграничение доступа к защищаемым данным на рабочей станции и на файловом сервере;

5) создание замкнутой программной среды разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках;

6) защита от воздействия вредоносных программ;

7) контроль целостности модулей системы защиты, системных областей диска и произвольных списков файлов в автоматическом режиме и по командам администратора;

8) регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

9) централизованный сбор, хранение и обработка на файловом сервере журналов регистрации рабочих станций сети;

10) защита данных системы защиты на файловом сервере от доступа всех пользователей, включая администратора сети;

11) централизованное управление настройками средств разграничения доступа на рабочих станциях сети;

12) оповещение администратора безопасности обо всех событиях НСД, происходящих на рабочих станциях;

13) оперативный контроль за работой пользователей сети, изменение режимов функционирования рабочих станций и возможность блокирования (при необходимости) любой станции сети.

136.Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

1) физическая целостность всех компонентов ИС Товарищества обеспечена;

2) каждый сотрудник (пользователь системы) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

3) использование на рабочих станциях ИС Товарищества инструментальных и технологических программ (тестовых утилит, отладчиков и т.п.), позволяющих предпринять попытки взлома или обхода средств защиты, ограничено и строго регламентировано;

4) в защищенной системе нет программирующих пользователей. Разработка и отладка программ осуществляется за пределами защищенной системы;

5) все изменения конфигурации технических и программных средств ПЭВМ ИС производятся строго в установленном порядке только на основании распоряжений руководства структурных подразделений Товарищества;

6) сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальные помещениях, шкафах, и т.п.).

7) специалистами, ответственными за обеспечение безопасности информации, осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7.3.1. Средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей

137.В целях предотвращения работы с ИС Товарищества посторонних лиц необходимо обеспечить возможность распознавания системой каждого законного пользователя (или ограниченных групп пользователей). Для этого в системе (в защищенном месте) должен храниться ряд признаков каждого пользователя, по которым этого пользователя можно опознать. В дальнейшем при входе в систему, а при необходимости - и при выполнении определенных действий в системе, пользователь обязан себя идентифицировать, т.е. указать идентификатор, присвоенный ему в системе. Кроме того, для идентификации могут применяться различного рода устройства: магнитные карточки, ключевые вставки, дискеты и т.п.

138.Аутентификация (подтверждение подлинности) пользователей должна осуществляться на основе использования паролей (секретных слов) или проверки уникальных характеристик (параметров) пользователей при помощи специальных биометрических средств.

7.3.2. Средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИС

139.После распознавания пользователя система должна осуществлять авторизацию пользователя, то есть определять, какие права предоставлены пользователю: какие данные и как он может использовать, какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т.п. Авторизация пользователя должна осуществляется с использованием следующих механизмов реализации разграничения доступа:

1) механизмов избирательного управления доступом, основанных на использовании атрибутных схем, списков разрешений и т.п.;

2) механизмов полномочного управления доступом, основанных на использовании меток конфиденциальности ресурсов и уровней допуска пользователей;

3) механизмов обеспечения замкнутой среды доверенного программного обеспечения (индивидуальных для каждого пользователя списков разрешенных для запуска программ), поддерживаемых механизмами

идентификации (распознавания) и аутентификации (подтверждения подлинности) пользователей при их входе в систему.

140.Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

141.Технические средства разграничения доступа должны быть составной частью единой системы контроля доступа:

1) на контролируемую территорию;
2) в отдельные помещения;
3) к элементам ИС и элементам системы защиты информации (физический доступ); к ресурсам ИС (программно-математический доступ);
4) к информационным хранилищам (носителям информации, томам, файлам, наборам данных, архивам, справкам, записям и т.д.);
5) к активным ресурсам (прикладным программам, задачам, формам запросов и т.п.); к операционной системе, системным программам и программам защиты и т.п.

7.3.3. Средства обеспечения и контроля целостности программных и информационных ресурсов

142.Контроль целостности программ, обрабатываемой информации и средств защиты, с целью обеспечения неизменности программной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной корректировки информации должен обеспечиваться:

1) средствами подсчета контрольных сумм; средствами электронной цифровой подписи;
2) средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
3) средствами разграничения доступа (запрет доступа с правами модификации или удаления).

143.В целях защиты информации и программ от несанкционированного уничтожения или искажения необходимо обеспечить:

1) дублирование системных таблиц и данных;
2) дуплексирование и зеркальное отображение данных на дисках;
3) отслеживание транзакций;
4) периодический контроль целостности операционной системы и пользовательских про грамм, а также файлов пользователей;
5) антивирусный контроль;
6) резервное копирование данных по заранее установленной схеме;
7) хранение резервных копий вне помещения файл-сервера;
8) обеспечение непрерывности электропитания для файл-серверов и критичных рабочих станций и кондиционирование электропитания для остальных станций сети.

7.3.4. Средства оперативного контроля и регистрации событий безопасности

144.Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций. Средства контроля и регистрации должны предоставлять возможности:

1) ведения и анализа журналов регистрации событий безопасности (системных журналов). Журналы регистрации должны вестись для каждой рабочей станции сети;

2) оперативного ознакомления администратора безопасности с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД;

3) получения твердой копии (печати) системного журнала;

4) упорядочения системных журналов по дням и месяцам, а также установления ограничений на срок их хранения;

5) оперативного оповещения администратора безопасности о нарушениях.

145.При регистрации событий безопасности в системном журнале должна фиксироваться следующая информация:

1) дата и время события;

2) идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;

3) действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

146.Средства контроля должны обеспечивать обнаружение и регистрацию следующих событий:

1) вход пользователя в систему;

2) вход пользователя в сеть;

3) неудачная попытка входа в систему или сеть (неправильный ввод пароля);

4) подключение к файловому серверу;

5) запуск программы;

6) завершение программы;

7) оставление программы резидентно в памяти;

8) попытка открытия файла недоступного для чтения;

9) попытка открытия на запись файла недоступного для записи;

10) попытка удаления файла недоступного для модификации;

11) попытка изменения атрибутов файла недоступного для модификации;

12) попытка запуска программы, недоступной для запуска;

13) попытка получения доступа к недоступному каталогу;

14) попытка чтения/записи информации с диска, недоступного пользователю;

15) попытка запуска программы с диска, недоступного пользователю;

16) нарушение целостности программ и данных системы защиты;

17) и др.

147.Должны поддерживаться следующие основные способы реагирования на обнаруженные факты НСД:

1) извещение владельца информации о НСД к его данным;

2) снятие программы (задания) с дальнейшего выполнения;

3) извещение администратора баз данных и администратора безопасности;

4) отключение терминала (рабочей станции), с которого были осуществлены попытки НСД к информации;

5) исключение нарушителя из списка зарегистрированных пользователей; подача сигнала тревоги и др.

7.3.5. Криптографические средства защиты информации

148.Одним из важнейших элементов системы обеспечения безопасности информации ИС Товарищества должно быть использование криптографических методов и средств защиты информации от несанкционированного доступа при ее передаче по каналам связи.

149.Все средства криптографической защиты информации в ИС Товарищества должны строиться на основе базисного криптографического ядра, прошедшего всесторонние исследования специализированными организациями. На использование криптографических средств Товарищество должно иметь лицензию.

150.Ключевая система применяемых в ИС Товарищества шифровальных средств должна обеспечивать криптографическую живучесть и многоуровневую защиту от компрометации ключевой информации, разделение пользователей по уровням обеспечения защиты и зонам их взаимодействия между собой и пользователями других уровней.

151.Конфиденциальность и имитозащита информации при ее передаче по каналам связи должна обеспечиваться за счет применения в системе шифросредств абонентского и на отдельных направлениях канального шифрования. Сочетание абонентского и канального шифрования информации должно обеспечивать ее сквозную защиту по всему тракту про хождения, защищать информацию в случае ее ошибочной переадресации за счет сбоев и неисправностей аппаратно-программных средств центров коммутации.

152.В ИС Товарищества, являющейся системой с распределенными информационными ресурсами, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений. При этом должны использоваться только стандартизованные алгоритмы цифровой подписи, а

соответствующие средства, реализующие эти алгоритмы, должны быть сертифицированы.

7.4. Защита информации от утечки по техническим каналам

153.В качестве основных мер защиты информации, циркулирующей в ИС Товарищества, рекомендуются:

1) использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, а также образцов технических средств, прошедших специальные исследования, в соответствии с требованиями предписания на эксплуатацию;

2) использование сертифицированных средств защиты информации;

3) размещение объекта защиты относительно границы контролируемой зоны с учетом радиуса зоны возможного перехвата информации, полученного для данного объекта по результатам специальных исследований;

4) маскирующее зашумление побочных электромагнитных излучений и наводок информативных сигналов;

5) конструктивные доработки технических средств и помещений, где они расположены, в целях локализации возможных каналов утечки информации;

6) размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах контролируемой зоны;

7) развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

8) периодическая проверка технических средств на отсутствие паразитной генерации их элементов;

9) создание выделенных сетей связи и передачи данных с учетом максимального затруднения доступа к ним посторонних лиц;

10) развязка линий связи и других цепей между выходящими за пределы контролируемой зоны и находящимися внутри нее;

11) использование защищенных каналов связи;

12) проверка технических средств перед введением в эксплуатацию на отсутствие в них электронных устройств перехвата информации.

154.Обеспечение защиты информации от утечки по техническим каналам при ее обработке (обсуждении), хранении и передаче по каналам связи предусматривает:

1) предотвращение утечки обрабатываемой техническими средствами информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований, создаваемых функционирующими техническими средствами;

2) предотвращение утечки информации в линиях связи, а также при ведении конфиденциальных переговоров;

155.Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется путем применения защищенных технических средств, сертифицированных по требованиям безопасности информации, внедрением объектовых мер защиты, в том числе установлением контролируемой зоны вокруг объектов ИС Товарищества, средств активного противодействия (при необходимости) и др. Конкретные требования к мерам объектовой защиты определяются по результатам специальных исследований технических средств с учетом установленной категории защищаемого объекта в зависимости от степени конфиденциальности обрабатываемой информации и условий ее размещения.

156.Исключение перехвата техническими средствами речевой информации достигается проектными решениями, обеспечивающими необходимую звукоизоляцию помещений, применением технических средств и организационных мер защиты оборудования, расположенного в помещениях.

157.Основными направлениями снижения уровня и информативности ПЭМИН являются:

1) разработка и выбор оптимальных схем и элементов, основанных на применении устройств с низким уровнем излучения типа:

жидкокристаллических и газоразрядных экранов отображения;

оптико-электронных и волоконно-оптических линий передачи данных;

запоминающих устройств на магнитных доменах, голографических запоминающих устройств и т.п.;

2) экранирование (развязка) отдельных элементов и устройств ИС, реализуемое путем:

локального экранирования излучающих элементов СВТ и средств связи;

экранирование кабелей и устройств заземления;

применение развязывающих фильтров в цепях питания и т.п.;

3) использование специальных программ и кодов, базирующихся:

на применении мультипрограммных режимов обработки данных, обеспечивающих минимальные интервалы обращения к защищаемой информации;

на применении параллельных многоразрядных кодов, параллельных кодов с малой избыточностью, а также симметричных кодов;

на ограничении регулярности вывода и времени отображения информации на устройствах отображения;

4) применение активных мешающих воздействий, основанных на использовании встроенных синхронизированных генераторов:

генераторов импульсных помех;

специальных (инверсных) схем заполнения интервалов;

5) использование специальных схем нарушения регулярности вывода информации на устройства отображения.

7.5. Защита речевой информации при проведении переговоров

158.Исходя из возможности перехвата речевой информации при проведении разговоров конфиденциального характера с помощью внедрения специальных электронных устройств, транслирующих эту информацию, акустических, виброакустических и лазерных технических средств, информации, наведенной на различные электрические и прочие цепи, выходящие за пределы контролируемой зоны, противодействие этим угрозам безопасности информационных ресурсов должно осуществляться всеми доступными средствами и методами.

159.Помещения должны быть проверены на предмет отсутствия в них (в стеновых панелях, фальшполах и фальшпотолках, мебели, технических средствах, размещенных в этих помещениях) закладных устройств, технические средства передачи информации (телефоны, телефаксы, модемы), а также различные электрические и прочие цепи, трубопроводы, системы вентиляции и кондиционирования и т.д. должны быть защищены таким образом, чтобы акустические сигналы не могли быть перехвачены за пределами контролируемой зоны, а в необходимых случаях и за пределами данного выделенного помещения.

160.В этих целях используются проектные решения, обеспечивающие звукоизоляцию помещений, специальные средства обнаружения закладных устройств, устанавливаются временные или постоянные посты радио контроля, на технические средства передачи информации устанавливаются устройства, предотвращающие перехват акустических сигналов с линий связи, на электрические цепи, выходящие за пределы контролируемой зоны, ставятся фильтры, а на трубопроводы диэлектрические вставки, используются системы активной защиты в акустическом и других диапазонах.

7.6. Управление системой обеспечения безопасности информации

161.Управление системой обеспечения безопасности информации в ИС представляет собой целенаправленное воздействие на компоненты системы обеспечения безопасности (организационные, технические, программные и криптографические) с целью достижения требуемых показателей и норм защищенности циркулирующей в ИС Товарищества информации в условиях реализации основных угроз безопасности.

162.Главной целью организации управления системой обеспечения безопасности информации является повышение надежности защиты информации в процессе ее обработки, хранения и передачи.

163.Целями управления системой обеспечения безопасности информации являются:

1) на этапе создания и ввода в действие ИС Товарищества - разработка и реализация научно-технических программ и координационных планов создания внутренних актов и технической базы, обеспечивающей использование передовых зарубежных средств и информационных

технологий и производство отечественных технических и программных средств обработки и передачи информации в защищенном исполнении в интересах обеспечения безопасности информации ИС; организация и координация взаимодействия в этой области разработчиков ИС, концентрация кадровых, финансовых и иных ресурсов заинтересованных сторон при разработке и поэтапном вводе в действие системы; создание действенной организационной структуры, обеспечивающей комплексное решение задач безопасности информации при функционировании ИС, в том числе службы безопасности ИС, оснащенной необходимыми программно-аппаратными средствами управления и контроля;

2) на этапе эксплуатации ИС - обязательное и неукоснительное выполнение предусмотренных на этапе создания ИС правил и процедур, направленных на обеспечение безопасности информации, всеми задействованными в системе участниками, эффективное пресечение посягательств на информационные ресурсы, технические средства и информационные технологии, своевременное выявление негативных тенденций и совершенствование управления в области защиты информации.

164.Управление системой обеспечения безопасности информации реализуется специализированной подсистемой, представляющей собой совокупность технических, программных и криптографических средств и организационных мероприятий и взаимодействующих друг с другом пунктов управления различных уровней.

165.Ответственными за управление системой обеспечения защиты информации в информационных системах Товарищества являются сотрудники, наделенные соответствующими функциональными обязанностями (системные администраторы).

166.Функциями подсистемы управления являются: информационная, управляющая и вспомогательная.

167.Информационная функция заключается в непрерывном контроле состояния системы защиты, проверке соответствия показателей защищенности допустимым значениям и немедленном информировании операторов безопасности о возникающих в ИС ситуациях, способных привести к нарушению безопасности информации. К контролю состояния системы защиты предъявляются два требования: полнота и достоверность. Полнота характеризует степень охвата всех средств защиты и параметров их функционирования. Достоверность контроля характеризует степень адекватности значений контролируемых параметров их истинному значению. В результате обработки данных контроля формируется информация состояния системы защиты, которая обобщается (агрегируется) и передается на вышестоящие пункты управления.

168.Управляющая функция заключается в формировании планов реализации технологических операций ИС с учетом требований безопасности информации в условиях, сложившихся для данного момента времени, а

также в определении места возникновения ситуации уязвимости информации и предотвращении ее утечки за счет оперативного блокирования участков ИС, на которых возникают угрозы безопасности информации. К управляющим функциям структурного подразделения, ответственного за организацию защиты информации в информационной системе относятся учет, хранение, и выдача документов и информационных носителей, паролей и ключей. При этом генерация паролей, ключей, сопровождение средств разграничения доступа, приемка включаемых в программную среду ИС новых программных средств, контроль соответствия программной среды эталону, а также контроль за ходом технологического процесса обработки защищаемой информации возлагается на подразделение обеспечивающее защиту информации в информационных системах.

169.К вспомогательным функциям подсистемы управления относятся учет всех операций, выполняемых в ИС с защищаемой информацией, формирование отчетных документов и сбор статистических данных с целью анализа и выявления потенциальных каналов утечки информации.

7.7. Контроль эффективности системы защиты

170.Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации за счет несанкционированного доступа к ней, а также предупреждения специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

171.Контроль должен осуществляться подразделением по организации защиты информации в информационной системе (оперативный контроль в процессе информационного взаимодействия в ИС) с помощью штатных средств системы защиты информации от НСД и специальных программных средств контроля.

172.Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.