Защищенная система электронного документооборота подразделений ОВД.

Оглавление

[Введение 5](#_Toc290558139)

[1 ОСНОВЫ РАБОТЫ ЗАЩИЩЕННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 8](#_Toc290558140)

[1.1 Понятие, задачи, функции защищенной системы электронного документооборота 8](#_Toc290558141)

[1.2 Нормативно-правовое регулирование функционирования защищенной системы электронного документооборота 11](#_Toc290558142)

[Выводы: 19](#_Toc290558143)

[2 ОСОБЕННОСТИ ЗАЩИЩЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 21](#_Toc290558144)

[2.1 Основные угрозы безопасности систем электронного документооборота 21](#_Toc290558145)

[2.2 Методы обеспечения безопасности информации в системах электронного документооборота 28](#_Toc290558146)

[Выводы: 38](#_Toc290558147)

[3 ПРИМЕНЕНИЕ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ПОДРАЗДЕЛЕНИЯХ ОВД 39](#_Toc290558148)

[3.1 Анализ существующего электронного документооборота в подразделениях ОВД 39](#_Toc290558149)

[3.2 Основы документооборота в деятельности ОВД 39](#_Toc290558150)

[3.3 Выбор и обоснование методов защиты систем электронного документооборота 49](#_Toc290558151)

[3.3.1 Аутентификация 49](#_Toc290558152)

[3.3.2 Межсетевое экранирование 52](#_Toc290558153)

[3.4 Выбор и обоснование программных и аппаратных средств для обеспечения защиты систем электронного документооборота 58](#_Toc290558154)

[3.4.1 Выбор персонального брандмауэра 58](#_Toc290558155)

[3.4.2 Выбор дополнительного средства аутентификации 63](#_Toc290558156)

[Выводы: 65](#_Toc290558157)

[Заключение 66](#_Toc290558158)

[Список использованной литературы 67](#_Toc290558159)

# Введение

Информационная безопасность – одно из популярнейших сегодня понятий. Наша жизнь уже неразрывно связана с информационными технологиями в современном их понятии, и поэтому защищать свои данные уже приходится каждому из нас. Одно из основных направлений в обеспечении информационной безопасности – это безопасность в сфере образования, так как именно в образовательных учреждениях этот вопрос стоит наиболее остро.

Информация и обеспечивающие ее системы и сети являются ценными ресурсами. Собственники информации сталкиваются с возрастающей угрозой нарушения режима безопасности, исходящей из различных источников. Информационным системам и сетям могут угрожать такие опасности, как: компьютерное мошенничество, компьютерные вирусы, хакеры, вандализм, хищение, разглашение конфиденциальной информации и другие виды угроз. В процентном отношении, по различным оценкам специалистов, данные угрозы в среднем распределяются следующим образом:

* разглашение информации в результате подкупа работников – 43%;
* копирование программ и данных – 24%;
* проникновение в ПЭВМ – 18%;
* подслушивание переговоров – 5%.

Анализ состояния дел в области информационной безопасности позволяет сделать вывод, что система мер, обеспечивающая защиту информации, значительно уменьшает возможность ее утечки, несанкционированного доступа, разглашения и потери информации. Главным является обеспечение бесперебойной работы организации и сведение к минимуму ущерба от событий, таящих угрозу информационной безопасности.

Этот вопрос напрямую касается и систем электронного документооборота как одной из составляющих информационной системы органов внутренних дел.

Внедрение систем электронного документооборота в органах МВД только начинается.

К примеру, в рамках проведения опытно-конструкторской работы по созданию единой автоматизированной информационной системы обеспечения деятельности штабных подразделений МВД России, отвечающей требованиям корпоративных стандартов и технологий ЕИТКС ОВД, специалистами компании «Электронные офисные системы» (ЭОС) была проведена адаптация и внедрение систем «ДЕЛО» и «eDocLib» в Организационно-инспекторском департаменте МВД России (ОИД МВД). Также, в рамках проекта, была проведена разработка и внедрение специализированной подсистемы автоматизации контроля исполнения документов, планов и поручений.

Выбор «ДЕЛО» и «eDocLib» был обусловлен надежностью, легкостью освоения, внедрения и сопровождения этих систем, успешным опытом предыдущих внедрений, в том числе и в структурах МВД, их соответствием российским стандартам документооборота, а также поддержкой ведомственных стандартов.

По итогам реализации проекта и первых месяцев работы внедренных систем, руководство ОИД МВД отмечает, что сотрудники ЭОС зарекомендовали себя квалифицированными специалистами, способными качественно решать любые задачи.

За пятнадцатилетнюю историю ЭОС, специалистами компании накоплен уникальный опыт по внедрению и адаптации систем автоматизации документооборота в крупнейших государственных и коммерческих структурах России, а ключевые специалисты ЭОС являются ведущими отечественными экспертами в области современных документационных технологий.

Министр внутренних дел Рашид Нургалиев, выступая на расширенном заседании коллегии министерства 22 марта 2011 года, заявил о том, что МВД России в ближайшее время планирует полностью перейти на электронный документооборот. В связи с этим становится более насущным вопрос обеспечения информационной безопасности при организации документооборота.

Целью данной дипломной работы является рассмотрение существующих угроз информационной безопасности систем электронного документооборота, их анализ и предложение мероприятия по по повышению их защищенности.

В соответствии с целью, в дипломной работе ставятся следующие задачи:

* исследование функций и задач, решаемых системами электронного документооборота;
* определение основных угроз безопасности систем электронного документооборота;
* определение основных методов обеспечения информационной безопасности систем электронного документооборота;
* формирование предложений по повышению защищенности систем электронного документооборота.

# ОСНОВЫ РАБОТЫ ЗАЩИЩЕННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

## **Понятие, задачи, функции защищенной системы электронного документооборота**

Система электронного документооборота (СЭД) - это система автоматизации работы с информационными документами на протяжении всего их жизненного цикла (создание, изменение, хранение, поиск, классификация и пр.), а также процессов взаимодействия между сотрудниками. При этом под документами в первую очередь подразумеваются неструктурированные электронные документы (файлы Word, Excel и пр.). Как правило, СЭД включает в себя электронный архив документов и систему автоматизации деловых процессов и поддержку функциональности делопроизводства.

Главное назначение СЭД — это организация хранения электронных документов, а также работы с ними (в частности, их поиска как по атрибутам, так и по содержимому). В СЭД должны автоматически отслеживаться изменения в документах, сроки исполнения документов, движение документов, а также контролироваться все их версии и подверсии. Комплексная СЭД должна охватывать весь цикл делопроизводства предприятия или организации — от постановки задачи на создание документа до его списания в архив, обеспечивать централизованное хранение документов в любых форматах, в том числе, сложных композиционных документов. СЭД должны объединять разрозненные потоки документов территориально удаленных предприятий в единую систему. Они должны обеспечивать гибкое управление документами как с помощью жесткого определения маршрутов движения, так и путем свободной маршрутизации документов. В СЭД должно быть реализовано жесткое разграничение доступа пользователей к различным документам в зависимости от их компетенции, занимаемой должности и назначенных им полномочий. Кроме того, СЭД должна настраиваться на существующую организационно-штатную структуру и систему делопроизводства предприятия, а также интегрироваться с существующими корпоративными системами.

Основными пользователями СЭД являются крупные государственные и коммерческие организации и предприятия, чья деятельность сопровождается большим объёмом создаваемых, обрабатываемых и хранимых документов.

Системы документооборота обычно внедряются, чтобы решать определенные задачи, стоящие перед организацией, из которых наиболее часто встречаются следующие:

* обеспечение более эффективного управления за счет автоматического контроля выполнения, прозрачности деятельности всей организации на всех уровнях.
* поддержка системы контроля качества, соответствующей международным нормам.
* поддержка эффективного накопления, управления и доступа к информации и знаниям. Обеспечение кадровой гибкости за счет большей формализации деятельности каждого сотрудника и возможности хранения всей предыстории его деятельности.
* протоколирование деятельности предприятия в целом (внутренние служебные расследования, анализ деятельности подразделений, выявление "горячих точек" в деятельности).
* оптимизация бизнес-процессов и автоматизация механизма их выполнения и контроля.
* исключение или максимально возможное сокращение оборота бумажных документов на предприятии. Экономия ресурсов за счет сокращения издержек на управление потоками документов в организации.
* Исключение необходимости или существенное упрощение и удешевление хранения бумажных документов за счет наличия оперативного электронного архива.

При выборе системы электронного документооборота принимаются во внимание следующие факторы:

* Требования по объему хранения. При наличии большого количества документов (по объему хранения), необходимо выбрать систему, поддерживающую иерархическое структурное хранение (HSM - Hierarchal Storage Management). Этот механизм хранит наиболее активно используемые данные на наиболее быстрых, но и наиболее дорогих носителях, в то время как реже используемая информация автоматически переносится на медленные и дешевые носители.
* Наличие формализуемых процедур, требующих поддержки их выполнения и автоматизации контроля (подготовки документов определенного типа, выполнения стандартных функций организации и т. д.).
* Необходимость автоматизации административного управления организацией. Степень сложности организационной структуры.
* Наличие территориально распределенных подразделений. Этот фактор накладывает определенные требования к удаленному доступу, к репликации данных и т.д.
* Наличие бумажного архива большого объема. Некоторые системы документооборота поставляются с уже интегрированными подсистемами массового ввода документов.
* Наличие не удовлетворяющей текущим потребностям системы документооборота.
* Необходимость в развитой маршрутизации документов, в управлении потоками работ (workflow managing). Как продолжение этой необходимости - потребность в поддержке произвольных бизнес-процессов, возможно работающих совместно с прикладными системами поддержки этих процессов.
* Требования по срокам хранения документов. При больших сроках хранения (десятки лет) стоит серьезно подумать об организации параллельного архива на микрофильмах.
* Требования к "открытости", расширяемости системы. Возможность интеграции с существующими информационными системами и использования имеющегося оборудования.
* Необходимость хранения изображений документов. Использование в организации специфических форматов хранения документов. Необходимость поддержки инженерных и конструкторских задач, других особенностей деятельности предприятия.
* Необходимость развитых средств поиска информации. Полная поддержка системой языков имеющихся в организации документов.
* Требования к безопасности (шифрование, организация доступа и т. д.). Возможность использования уже имеющихся в информационной инфраструктуре организации механизмов доступа в системе документооборота.
* Требования по соответствию определенным стандартам: внутренним, отраслевым, ГОСТ, международным стандартам по контролю качества, уровню организации хранения информации.

## **Нормативно-правовое регулирование функционирования защищенной системы электронного документооборота**

Правовую основу обеспечения информационной безопасности в Российской Федерации составляют Конституция Российской Федерации, Гражданский Кодекс Российской Федерации, Уголовный Кодекс Российской Федерации, а также следующие Федеральные законы, указы президента и постановления правительства:

* Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности»
* Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»
* Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
* Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»
* Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
* Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»
* Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
* Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
* Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»
* Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"»
* Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
* Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»
* Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 « Об организации лицензирования отдельных видов деятельности»
* Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
* Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 «О лицензировании деятельности но разработке и (или) производству средств защиты конфиденциальной информации»

Основные положения государственной политики в сфере обеспечения информационной безопасности изложены в Концепции национальной безопасности Российской Федерации и Доктрине информационной безопасности Российской Федерации.

Согласно Доктрине информационной безопасности Российской Федерации выделены четыре основные составляющие национальных интересов РФ в информационной сфере:

* обеспечение конституционных прав и свобод человека и гражданина на личную и семейную тайны, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
* укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности, создание условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации
* запрещение сбора, хранения, использования и распространения информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством;
* защита информационных ресурсов от несанкционированного доступа (НСД), обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Конституцией Российской Федерации определено, что мероприятия по защите информации не должны прямо или косвенно влиять на частную жизнь сотрудников, вне рамок, определенных служебными обязанностями. Не допускается сбор сведений о частной жизни сотрудников, ознакомление с их перепиской.

Гражданский кодекс Российской Федерации определяет, что объектом права являются (ст. 128) — «...информация, результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)». Кроме этого определяются понятия служебной и коммерческой тайны (ст. 139), определяются характерные признаки, присущие сведениям, составляющим служебную и коммерческую тайну. Кроме этого устанавливается, что «лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну, вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору». Статьей 727 устанавливается, что сторона, которая получила от другой стороны информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, которые могут рассматриваться как коммерческая тайна, не вправе сообщать ее третьим лицам без согласия другой стороны.

Уголовным Кодексом Российской Федерации предусматривается уголовная ответственность, которая может, в том числе, распространяться на сотрудников ОВД при:

* сборе или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия (ст.137);
* нарушении тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, в том числе, совершенное лицами с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации (ст.13 8);
* нарушении авторских и смежных прав, нарушении изобретательских и патентных прав (ст.146, ст. 147);
* незаконном получении или разглашении сведений, составляющих коммерческую или банковскую тайну (ст.183);
* неправомерном доступе к охраняемой законом компьютерной информации (ст. 272);
* создании, использовании и распространении вредоносных программ для ЭВМ (ст.273);
* нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.273).

Закон «О безопасности», закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции и устанавливающие порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации, регулируются законом «Об информации, информатизации и защите информации».

Данный закон наряду с другими вводит очень важное понятие - понятие конфиденциальной информации. Одновременно данный закон рассматривает вопросы создания и использования информационных технологий и средств их обеспечения, а также защиты информации и прав субъектов, участвующих в информационных процессах и информатизации.

Указ Президента Российской Федерации № 188 от 06.03.97 «Об утверждении перечня сведений конфиденциального характера» закрепляет перечень сведений конфиденциального характера. К подобным сведениям, в том числе, относятся:

* сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

Федеральный закон РФ «О связи» устанавливает понятие тайны связи и сведения, к ней относящиеся. Закон определяет обязательства операторов связи по защите сведений, передаваемых по предоставляемым каналам связи.

Целью Федерального закона "Об электронной цифровой подписи" от 10 января 2002 года № 1-ФЗ является обеспечение правовых условий использования электронной цифровой подписи (ЭЦП) в электронных документах, при соблюдении которых ЭЦП в электронном документе признаётся равнозначной собственноручной подписи в документе на бумажном носителе.

Закон «Об участии в международном информационном обмене» обеспечивает создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиту интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене, защиту интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

Федеральный закон «О техническом регулировании», вступивший в силу с 1 июля 2003 года, который открывает новые возможности технического регулирования. В соответствии с этим законом возможность жесткого государственного регулирования в сфере защиты информации резко уменьшилась и теперь может осуществляться лишь посредством требований, изложенных в технических регламентах, представляющих собой «документы, которые приняты международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации и устанавливают обязательные для применения и исполнения требования к объектам технического регулирования».

Нормативно-методическую базу, определяющую требования и рекомендации к защите информации в автоматизированных системах, составляют руководящие документы Гостехкомиссии России, ФСБ России и государственные стандарты.

Наиболее известными и применяемыми в международной практике стандартами являются:

* Международный стандарт безопасности информационных систем ISO/IEC 17799 "Управление информационной безопасностью";
* Международный стандарт ISO/IEC 15408-1:1999 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий";
* Стандарт CobiT - "Контрольные Объекты для Информационной и смежных Технологий".

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

* Необходимость обеспечения информационной безопасности;
* Основные понятия и определения информационной безопасности;
* Политика информационной безопасности компании;
* Организация информационной безопасности на предприятии;
* Классификация и управление корпоративными информационными ресурсами;
* Кадровый менеджмент и информационная безопасность;
* Физическая безопасность;
* Администрирование безопасности корпоративных информационных систем;
* Управление доступом;
* Требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
* Управление бизнес-процессами компании с точки зрения информационной безопасности;
* Внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 "Спецификации систем управления информационной безопасностью - Information security management - Part 2: Specification for information security management systems", определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Сущность аудита безопасности на соответствие системы управления информационной безопасностью компании требованиям стандарта заключается в проверке выполнения каждого положения стандарта ISO 17799. По каждому такому положению проверяющие должны ответить на два вопроса: выполняется ли данное требование, и если нет, то каковы причины невыполнения? На основе ответов составляется Ведомость соответствия, основная цель которой - аргументированное обоснование имеющихся отклонений информационной безопасности от требований стандарта ISO 17799. По завершению аудита безопасности выявленные несоответствия при необходимости могут быть устранены. Другими словами, в ходе выполнения аудита всей компании в целом, аудитор, выполняющий данную работу, должен собрать доказательства того, что компания отвечает всем требованиям стандарта ISO 17799. Это делается на основе анализа документов, бесед с экспертами, а при необходимости и проведения соответствующих организационных проверок режима безопасности и инструментальных проверок компонентов корпоративной системы Internet/Intranet. В результате должны быть проверены: организация информационной безопасности компании, обязанности по обеспечению информационной безопасности сотрудников всех должностей, наличие документированной политики и стратегии информационной безопасности для компании, и, в частности, документированной стратегии и общих положений подхода к оцениванию и управлению рисками. При этом обращается внимание на наличие документированных, применимых на практике методик по оцениванию и управлению рисками, обоснования правильности выбора средств защиты для информационной системы компании. Попутно выявляется наличие документированных процедур оценки остаточного риска, проверки режима информационной безопасности, а также журналов, в которых фиксируются результаты проверки. У проверяющего аудитора должна быть полная ясность относительно наличия документированных правил обслуживания и администрирования информационной системы, наличие документированных распоряжений должностных лиц по проведению периодических проверок оценивания и управления рисками, документации по системе управления информационной безопасностью и реестра необходимых средств.

## Выводы:

Таким образом, совеменнные системы электронного документооборта являются сложными и многофункциональными программно-аппаратными комплексами, предназначенными в первую очередь для повышения удобства обработки и хранения различных документов. Требования к обеспечению защищенности СЭД рассматриваются в контексте требований к защищенности все информационной системы ОВД,

# ОСОБЕННОСТИ ЗАЩИЩЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

## Основные угрозы безопасности систем электронного документооборота

Угрозы для системы электронного документооборота достаточно стандартны и могут быть классифицированы следующим образом. Угроза целостности — повреждение и уничтожение информации, искажение информации — как не намеренное в случае ошибок и сбоев, так и злоумышленное. Угроза конфиденциальности — это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменения маршрутов следования. Угроза работоспособности системы — всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы; сюда входят как умышленные атаки, так и ошибки пользователей, а также сбои в оборудовании и программном обеспечении.

Защиту именно от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота. При этом, с одной стороны, внедряя СЭД, упорядочивая и консолидируя информацию, увеличиваются риски реализации угроз, но с другой стороны, как это ни парадоксально, упорядочение документооборота позволяет выстроить более качественную систему защиты.

Все физические лица, имеющие доступ к ресурсам комплекса, могут быть отнесены к следующим категориям:

Внешние нарушители (категория I) – лица, не имеющие права доступа в КЗ, в которой располагаются ресурсы комплекса.

Внешний нарушитель не имеет непосредственного доступа к системе и ее ресурсам, находящимся в пределах контролируемой зоны комплекса. Этот нарушитель может осуществлять атаки только из вне контролируемой зоны.

Внутренние нарушители (категория II) – лица, имеющие право постоянного или разового доступа в КЗ, в которой располагаются ресурсы комплекса.

Все лица категории II могут быть отнесены к следующим классам:

* класс пользователей комплекса;
* класс лиц, не являющихся пользователями комплекса (обслуживающий персонал, сотрудники внешних организаций, привлекаемые к проведению работ пусконаладочных или ремонтных работ, другие лица, имеющие доступ в КЗ).

Предполагается, что лица входящие в группу администраторов не относятся к потенциальным нарушителям.

Класс пользователей комплекса может быть разделен на следующие виды:

* сотрудники 1;
* сотрудники 2;
* персонал, обеспечивающий эксплуатацию комплекса.

Сотрудники 1 являются высоко квалифицированными пользователями, но так как они в силу функциональных обязанностей имеют доступ практически к полному набору информации комплекса, то предполагается, что они не будут предпринимать попыток преодоления средств защиты и дополнительных средств защиты.

Сотрудники 2, обладающие навыками пользователей, являются сотрудниками органов. Предполагается, что данные пользователи не будут предпринимать попыток преодоления средств защиты и дополнительных средств защиты.

Внутренний нарушитель не может проводить атаку из-за пределов КЗ.

Сговор между внутренним и внешним нарушителями исключен организационными мерами.

Внутренний нарушитель скрывает свои несанкционированные действия от других сотрудников.

Работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций внутренних нарушителей.

Объекты атак совпадают с защищаемыми активами СЭД:

* информация пользователей комплекса на всех этапах ее обработки (хранимая, накапливаемая, обрабатываемая и служебная);
* средства и система защиты информации комплекса, включая ключевую, парольную и аутентифицирующую информацию;
* компоненты комплекса (программное обеспечение и технические средства).

Основными целями атак являются нарушения:

* конфиденциальности (защищённости от несанкционированного раскрытия информации об объекте атаки);
* целостности (защищённости от несанкционированной модификации объекта атаки);
* доступности (обеспечения своевременного санкционированного получения доступа к объекту атаки);
* достоверности (идентичности объекта атаки тому, что заявлено);
* подконтрольности (обеспечения того, что действия субъекта по отношению к объекту атаки могут быть прослежены уникально по отношению к субъекту).

Предположим, что нарушитель имеет:

* данные об организации работы, структуре и используемых технических, программных и программно-технических средствах комплекса;
* сведения об информационных ресурсах комплекса: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
* данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств комплекса (только для внешнего нарушителя);
* данные о реализованных в системе и средствах защиты принципах и алгоритмах;
* исходные тексты программного обеспечения комплекса;
* сведения о возможных каналах атак;
* информацию о способах атак.

Предполагается, что нарушитель не обладает информацией о ключевой, парольной и аутентифицирующей информации комплекса. При этом предполагается, что внутренний нарушитель обладает, в пределах своих полномочий, информацией о собственной ключевой, парольной и аутентифицирующей информации.

Предполагается, что с учётом режимных и организационно-технических мер исключен доступ внешнего нарушителя к коммутационному оборудованию, системам электропитания и заземления.

С учётом изложенного возможными каналами атак являются:

* каналы непосредственного доступа к объекту атаки (например, акустический, визуальный, физический);
* штатные средства комплекса;
* съемные МНИ;
* носители информации, выведенные из употребления;
* структурированная кабельная система;
* каналы распространения побочных сигналов, сопровождающих функционирование СВТ комплекса.

Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все средства, необходимые для проведения атак по доступным ему каналам атак.

Описание способов атак

Для комплекса определен следующий перечень способов атак:

Нарушитель может использовать следующие основные способы атак:

* перехват сведений о защищаемой информации, о комплексе и его компонентах, включая средства и систему защиты – только при нарушении политики безопасности;
* хищение производственных отходов (распечаток, записей, списанных носителей и т.п.) – только при нарушении политики безопасности;
* восстановление (в том числе и фрагментарное) защищаемой информации и информации о комплексе путем анализа выведенных из употребления и ставших после этого доступными нарушителю МНИ – только при нарушении политики безопасности;
* считывание или восстановление информации (в том числе и фрагментарное) по остаточным следам на носителях защищаемой информации, сданных в ремонт, на обслуживание, переданных для использования другими пользователями или для использования за пределами комплекса – только при нарушении политики безопасности;
* негласное (скрытое) временное изъятие съемных носителей защищаемой информации, аутентифицирующей или ключевой информации – только при нарушении политики безопасности;
* хищение съемных носителей защищаемой информации, аутентифицирующей или ключевой информации – только при нарушении политики безопасности;
* негласная (скрытая) модификация защищаемой информации, хранящейся на съемных носителях информации – только при нарушении политики безопасности;
* использование незарегистрированных носителей информации – только при нарушении политики безопасности;
* визуальный просмотр защищаемой информации на экране монитора – только при нарушении политики безопасности;
* ознакомление с распечатанной защищаемой информацией – только при нарушении политики безопасности;
* вывод информации на неучтенные носители (в том числе, вывод на печать), а также с нарушением требований руководящих и нормативных документов, регламентирующих порядок обращения с информацией соответствующей категории доступа – только при нарушении политики безопасности;
* перехват защищаемой информации из структурированной кабельной системы;
* целенаправленное искажение защищаемой информации в структурированной кабельной системе;
* навязывание ложной (специально сформированной нарушителем) информации через структурированную кабельную систему;
* перенаправление потоков данных путем воздействия через структурированную кабельную систему;
* нарушение связи между периферийными рабочими местами и центрами за счет преднамеренной загрузки трафика ложными сообщениями, приводящее к исчерпанию пропускной способности каналов связи структурированной кабельной системы;
* доступ к оставленным без присмотра функционирующим штатным средствам комплекса – только при нарушении политики безопасности;
* несанкционированное изменение конфигурации технических средств комплекса – только при нарушении политики безопасности;
* подбор аутентифицирующей информации пользователей – только при нарушении политики безопасности;
* несанкционированный доступ к защищаемой информации с использованием штатных средств комплекса;
* модификация ведущихся в электронном виде регистрационных протоколов (журналов регистрации);
* модификация технических средств комплекса – только при нарушении политики безопасности;
* модификация программных средств комплекса с использованием штатных средств, включая нелегальное внедрение и использование неучтенных программ – только при нарушении политики безопасности;
* модификация программных средств комплекса с использованием ПССИВ, размещенных на съемных МНИ;
* вызывание сбоев технических средств АС – только при нарушении политики безопасности;
* внесение неисправностей в технические средства АС – только при нарушении политики безопасности;
* утечка, модификация, блокирование или уничтожение защищаемой информации с использованием штатных средств;
* утечка, модификация, блокирование или уничтожение защищаемой информации с использованием ПССИВ, размещенных на съемных МНИ;
* блокирование или уничтожение технических, программных и программно-технических компонентов АС – только при нарушении политики безопасности;
* несанкционированный доступ к защищаемой информации в процессе ремонтных и регламентных работ – только при нарушении политики безопасности;
* получение защищаемой информации, в том числе ключевой, парольной и аутентифицирующей информации на основе перехвата и анализа побочных сигналов, сопровождающих функционирование СВТ комплекса.

## **Методы обеспечения безопасности информации в системах электронного документооборота**

Базовый элемент любой СЭД — документ, внутри системы это может быть файл, а может быть запись в базе данных. Говоря о защищенном документообороте, часто подразумевают именно защиту документов, защиту той информации, которую они в себе несут. В этом случае все сводится к уже банальной (хотя и не простой) задаче защиты данных от несанкционированного доступа.

Обеспечение информационной безопасности при обработке информации в СЭД происходит прежде всего за счет применения внутренних служб безопасности.

Служба защиты - совокупность механизмов, процедур и других управляющих воздействий, реализованных для сокращения риска, связанного  с угрозой. Например, службы идентификации и аутентификации (опознания) помогают сократить риск угрозы неавторизованного пользователя. Некоторые службы обеспечивают защиту от угроз, в то время как другие службы обеспечивают обнаружение реализации угрозы. Примером последних могут служить  службы регистрации или наблюдения. Далее более подробно рассмотрим следующие службы::

* идентификация и установление подлинности - является службой безопасности, которая помогает гарантировать, что в  СЭД работают только авторизованные лица.
* управление доступом - является службой безопасности, которая помогает гарантировать, что ресурсы СЭД используются разрешенным способом.
* конфиденциальность данных и сообщений - является службой безопасности, которая помогает гарантировать, что данные ЛВС, программное обеспечение и сообщения не раскрыты неавторизованным лицам.
* целостность данных и сообщений - является службой безопасности, которая помогает гарантировать, что данные СЭД, программное обеспечение и сообщения не изменены неправомочными лицами.
* контроль участников взаимодействия - является службой безопасности, посредством которой гарантируется, что объекты, участвующие во взаимодействии, не смогут отказаться от  участия в нем. В частности, отправитель не сможет отрицать посылку сообщения (контроль участников взаимодействия  с подтверждением отправителя) или получатель не сможет отрицать получение сообщения (контроль участников взаимодействия с подтверждением  получателя).
* регистрация и наблюдение - является службой безопасности, с помощью которой может быть прослежено использование всех  ресурсов  СЭД.

Идентификация и аутентификация

Первый шаг к обеспечению безопасности ресурсов СЭД - способность проверить личности пользователей. Процесс подтверждения(проверки) личности пользователя назван  установлением подлинности (аутентификацией). Аутентификация обеспечивает основу для эффективного функционирования  других мер и средств защиты, используемых в СЭД. Например, механизм регистрации позволяет получить информацию об использовании пользователями ресурсов СЭД, основанную на идентификаторе пользователя. Механизм управления доступом разрешает доступ к ресурсам СЭД, основываясь на идентификаторе пользователя. Оба эти средства защиты эффективны только при условии, что пользователь, использующий службу СЭД - действительный пользователь, которому назначен данный идентификатор пользователя

Идентификация требует, чтобы  пользователь был так или иначе известен СЭД. Она обычно основана на назначении пользователю  идентификатора пользователя. Однако СЭД не может доверять заявленному идентификатору  без подтверждения его подлинности. Установление подлинности возможно при наличии у пользователя, чего - нибудь уникального, что только пользователь имеет, чего - нибудь единственного, что только пользователь знает, или чего - нибудь, что делает пользователя уникальным. Чем больше количество таких уникальных вещей предоставлено пользователем СЭД, тем меньше риск, что  кто-то подменит законного пользователя.

Требование, определяющее необходимость аутентификации, должно существовать в большинстве  политик безопасности СЭД. Это требование может содержаться неявно в политике концептуального уровня, которая подчеркивает необходимость эффективного  управления доступом к информации и ресурсам СЭД, или может быть явно выражено в политике относительно СЭД,  в виде заявления, что все пользователи должны быть уникально идентифицированы и аутентифицированы.

В большинстве СЭД используется механизм идентификации и аутентификации на основе схемы идентификатор пользователя/пароль. Однако исследовательские работы детализируют степень простоты, с которой могут угадываться пароли. Надлежащий выбор пароля (компромисс между  легкостью для запоминания пользователем и трудностью для угадывания другим человеком) всегда был проблемой. Генераторы паролей, которые создают пароли, состоящие из произносимых слогов, позволяют создавать более запоминающиеся пароли, чем те, что создаются генераторами, которые производят просто строки из случайных символов. Программы проверки паролей - это программы, которые позволяют пользователю определить, являются ли новые пароли легкими для угадывания и поэтому недопустимыми. Механизмы с использованием только паролей, особенно те, которые передают по СЭД пароль в открытом виде(в незашифрованной форме) уязвимы с точки зрения наблюдения и перехвата. Если после рассмотрения всех вариантов аутентификации, политика СЭД определяет, что системы аутентификации только на основе паролей приемлемы, то самой важной мерой защиты становится надлежащее  управление созданием паролей, их хранением, слежением за истечением срока их использования, и удалением.

Механизмы блокировки для устройств СЭД, автоматизированных рабочих мест или ПК, которые требуют для разблокировки аутентификации пользователя, могут быть полезны для пользователей, кто должен часто оставлять рабочее место. Эти механизмы блокировки позволяют пользователям остаться зарегистрированными в СЭД и покидать их рабочие места (в течение определенного периода времени, не длиннее заданного), не делая при этом свое рабочее место потенциально доступным злоумышленникам.

Механизмы, которые обеспечивают пользователя информацией об использовании его регистрационного имени, могут предупредить пользователя, что его  имя использовалось необычным образом (например, возникли многократные ошибки при регистрации). Эти механизмы включают уведомления о дате, времени, и местоположении последнего успешного сеанса и числе предыдущих ошибок при регистрации. Типы механизмов защиты, которые могли бы быть реализованы, чтобы обеспечить службы идентификации и аутентификации, приведены в списке ниже:

* механизм, основанный на паролях,
* механизм, основанный на интеллектуальных картах
* механизм, основанный на биометрии,
* генератор паролей,
* блокировка с помощью пароля,
* блокировка клавиатуры,
* блокировка ПК или автоматизированного рабочего места,
* завершение соединения после нескольких ошибок при регистрации,
* уведомление пользователя о "последней успешной регистрации" и "числе ошибок при регистрации",
* механизм аутентификации пользователя в реальном масштабе времени,
* криптография с уникальными ключами для каждого пользователя.

Управление доступом

Эта служба защищает против неавторизованного использования ресурсов СЭД, и может быть обеспечена при помощи механизмов управления доступом и механизмов привилегий. Большая часть файловых серверов и многопользовательских автоматизированных рабочих мест в некоторой степени обеспечивают эту службу . Однако, ПК, которые монтируют тома файловых серверов, обычно не осуществляют такое управление доступом. Пользователи должны понимать, что файлы из смонтированных дисков, используемые на ПК, находятся под управлением доступом ПК. По этой причине важно использовать службы управления доступом, конфиденциальности и целостности для ПК в максимально возможном объеме.

Управление доступом может быть достигнуто при использовании дискреционного управления доступом или мандатного управления доступом. Дискреционное управление доступом - наиболее общий тип управления доступом, используемого в СЭД. Основной принцип этого вида защиты состоит в том, что индивидуальный пользователь или программа, работающая от имени пользователя, имеет возможность явно определить типы доступа, которые могут осуществить другие пользователи (или программы, выполняющиеся от их имени)  к информации, находящейся в ведении данного пользователя. Дискреционное управление доступом отличается от мандатной защиты, в том, что оно реализует решения по управлению доступом, принятые пользователем. Мандатное управление доступом реализуется на основе результатов сравнения  уровня допуска пользователя и степени конфиденциальности информации.

Существуют механизмы управления доступом, которые поддерживают степень детализации управления доступом на уровне следующих категорий:  владелец информации,  заданная группа пользователей и "мира" (всех других авторизованных пользователей). Это позволяет владельцу файла (или каталога) иметь права доступа, отличающиеся от прав всех других пользователей, и позволяет владельцу файла определить особые права доступа для указанной группы людей, а также для всех остальных.

Операционная система СЭД может поддерживать профили пользователя и списки возможностей или списки управления доступом для определения прав  доступа для большого количества отдельных пользователей и большого количества различных групп. Использование этих механизмов позволяет обеспечить большую гибкость в предоставлении различных прав доступа для различных пользователей, которые могут обеспечить более строгий контроль доступа к файлам (или каталогам). (Более гибкие механизмы предотвращают предоставление пользователю больших прав доступа, чем необходимо, частой проблемы при описанном выше трехуровневом подходе). Списки управления доступом определяют права доступа специфицированных пользователей и групп к данному файлу или каталогу. Списки возможностей и профили пользователя определяют файлы и каталоги, к которым можно обращаться данным пользователям (или пользователю).

Управление доступом пользователя может осуществляться на уровне каталогов или на уровне файлов. Управление доступом на уровне каталога приводит к  тому, что  права доступа для всех файлов в каталоге становятся одинаковыми .

Механизмы привилегий позволяют авторизованным пользователям игнорировать ограничения на доступ, или другими словами некоторым способом легально обходить управление доступом, чтобы выполнить какую-либо функцию, получить доступ к файлу, и т.д.. Типы механизмов защиты, которые могли бы быть использованы для обеспечения службы управления доступом, приведены в списке ниже:

* + механизм управления доступом, использующий права доступа (определяющий права владельца, группы и всех остальных пользователей),
  + механизм управления доступом, использующий списки управления доступом, профили пользователей и списки возможностей,
  + управление доступом, использующее механизмы мандатного управления доступом,
  + детальный механизм привилегий.

Конфиденциальность данных и сообщений

Служба конфиденциальности данных и сообщений может использоваться,  когда необходима секретность информации. Как передняя линия защиты, эта служба может включать в себя механизмы, связанные со службой управления доступом, но может также полагаться на шифрование для обеспечения большего сохранения тайны. Шифрование информации преобразует ее в непонятную форму, называемую шифротекстом, а расшифровывание преобразует информацию обратно в ее первоначальную форму. Критичная информация может храниться в шифрованной форме, в виде шифротекста. Таким образом, если служба управления доступом будет обойдена, к  файлу может быть осуществлен доступ, но информация будет все еще защищена, поскольку находится в зашифрованной форме. (Использование шифрования может быть критическим на ПК, которые не обеспечивают службу управления доступом как передней линии защиты.)

Очень трудно управлять неавторизованным доступом к трафику СЭД, когда он передается по СЭД. Использование шифрования сокращает риск какого-либо перехвата и чтения проходящих транзитом через СЭД сообщений, делая сообщения нечитабельными для тех , кто сможет перехватить их. Только авторизованный пользователь, который имеет правильный ключ, сможет расшифровать сообщение после  его получения.

Типы механизмов безопасности, которые могли бы быть реализованы, чтобы обеспечить службу конфиденциальности сообщений и данных, приведены в списке ниже.

Механизмы

* технология шифрования файлов и сообщений,
* защита резервных копий на лентах, дискетах, и т.д.,
* физическая защита физической среды СЭД и устройств,
* использование маршрутизаторов, которые обеспечивают фильтрацию для ограничения широковещательной передачи (или блокировкой, или маскированием содержания сообщения).

Целостность данных и сообщений

Служба целостности данных и сообщений помогает защитить данные и программное обеспечение на автоматизированных рабочих местах, файловых серверах и других компонентах СЭД от неавторизованной модификации. Неавторизованная модификация может быть намеренной или случайной. Эта служба может быть обеспечена при помощи криптографических контрольных сумм,  и очень детальных механизмов управления доступом и привилегий. Чем больше точность управления доступом или механизма привилегий, тем менее вероятна возможность неавторизованной или случайной модификации.

Служба целостности данных и сообщений также помогает гарантировать, что сообщение не изменено, не удалено или не добавлено любым способом в течение передачи. (Некорректная модификация пакета сообщения обрабатывается на уровне управления доступом к среде, осуществляемого в рамках протокола СЭД.) Большинство из методов защиты, доступных сегодня, не могут предотвратить модификацию сообщения, но они могут обнаружить модификацию сообщения (если сообщение не удалено полностью).

Также могут использоваться электронные подписи для обнаружения модификации данных или сообщений. Электронная подпись может быть создана при помощи криптографии с открытыми или секретными ключами. При использовании системы с открытыми ключами документы в компьютерной системе подписываются с помощью электронной подписи  путем применения секретного  ключа отправителя документа. Полученная электронная подпись и документ могут быть затем  сохранены или переданы. Подпись может быть проверена при помощи открытого ключа создателя документа. Если подпись подтверждается  должным образом, получатель может быть уверен в том, что документ был подписан с использованием секретного ключа его создателя и что сообщение не было изменено после того, как оно было подписано. Поскольку секретные ключи известны только их владельцам, это делает также возможным проверку личности отправителя сообщения третьим лицом. Поэтому электронная подпись обеспечивает две различных службы: контроль участников взаимодействия  и целостность сообщения. Типы механизмов защиты, которые могли бы быть реализованы, чтобы обеспечить службу целостности данных и сообщений, представлены в списке ниже.

Механизмы

* коды аутентификации сообщения, используемые для программного обеспечения или файлов,
* использование электронной подписи, основанной на секретных ключах,
* использование электронной подписи, основанной на открытых ключах,
* детальный механизм привилегий,
* соответствующее назначение прав при управлении доступом (то есть отсутствие ненужных разрешений на запись),
* программное обеспечение для обнаружения вирусов,
* бездисковые автоматизированные рабочие места (для предотвращения локального хранения программного обеспечения и файлов),
* автоматизированные рабочие места без накопителей для дискет или лент для предотвращения появления подозрительного программного обеспечения.

Контроль участников взаимодействия

Служба контроля участников взаимодействия помогает гарантировать, что субъекты взаимодействия  не смогут отрицать участие во всем взаимодействии или какой-либо его части. Когда главной функцией СЭД является  электронная почта, эта служба безопасности становится очень важной. Контроль участников взаимодействия с подтверждением отправителя  дает получателю некоторую степень уверенности в том, что сообщение действительно прибыло от названного отправителя. Службу контроля участников взаимодействия  можно обеспечить с помощью  криптографических методов с использованием открытых ключей, реализующих электронную подпись. Механизм защиты, который мог бы быть реализован для обеспечения службы контроля участников взаимодействия, приведен ниже.

Механизм

* + использование электронных подписей с открытыми ключами.

Регистрация и наблюдение

Эта служба исполняет две функции. Первая - обнаружение возникновения угрозы. Для всех обнаруженных случаев нарушения безопасности  должна иметься возможность проследить действия нарушителя во всех частях  системы, что зависит от масштабов регистрации. Например, в случае вторжения злоумышленника в систему, журнал должен указывать, кто проводил сеанс с системой в это время, все критичные файлы, для которых имелись аварийно завершившиеся попытки доступа, все программы, которые запускались, и т.д.. Он должен также указывать критичные файлы и программы, к которым были успешные обращения в этот период времени. Может оказаться уместным иметь в некоторых областях СЭД (автоматизированных рабочих местах, файловых серверах, и т.д.) какую-либо разновидность службы регистрации.

Вторая функция этой службы -  обеспечить системных и сетевых администраторов статистикой, которая показывает, что система и сеть в целом функционируют должным образом. Это может быть сделано при помощи механизма аудирования, который использует файл журнала  в качестве исходных данных и перерабатывает  его в информацию относительно использования системы и ее защиты. Могут также использоваться средства наблюдения за СЭД, которые помогали бы обнаружить проблемы с ее доступностью по мере их возникновения. Типы механизмов защиты, которые могли бы использоваться, чтобы обеспечить службу регистрации и наблюдения, приведены в списке ниже.

Механизмы

* регистрация информации о сеансах пользователей(включая исходящую машину, модем, и т.д.),
* регистрация изменений прав пользователей для управления доступом,
* регистрация использования критичных файлов,
* регистрация модификаций, сделанных в критическом программном обеспечении,
* использование инструментов управления трафиком СЭД,
* использование средств аудирования.

## Выводы:

Основной угрозой для информации, обрабатываемой и хранимой в СЭД является возможность несанкционированного доступа к системе с целью неправомерного ее использования. Таким образом, основные методы и способы повышения защищенности СЭД должны быть направлены на повышения защиты от несанкционированного доступа.

# ПРИМЕНЕНИЕ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ПОДРАЗДЕЛЕНИЯХ ОВД

## **Анализ существующего электронного** документооборота **в** подразделениях **ОВД**

## **Основы документооборота в деятельности ОВД**

Документооборот - это движение документов в органе внутренних дел с момента их подготовки или получения документа до завершения его исполнения, отправки или сдачи в подразделение специальных фондов.

Электронные документы участвуют в документообороте органов внутренних дел наравне с бумажными документами.

Порядок прохождения документов и операции, производимые с ними в органах внутренних дел, регламентируются Инструкцией по документационному обеспечению и Регламентом внутренней организации Министерства внутренних дел Российской Федерации, утвержденным приказом МВД России от 30 декабря 2005 г. № 1167 , статусными документами органов внутренних дел, положениями о структурных подразделениях органов внутренних дел и должностными инструкциями их сотрудников.

Рациональный документооборот организуется на основании следующих положений:

* движение документов должно соответствовать процессам подготовки или исполнения документов, основанным на распределении функциональных обязанностей между исполнителями.
* маршруты прохождения однотипных документов должны быть унифицированы.

Учет входящих, подготовленных (исходящих, внутренних) документов в зависимости от документооборота производится в журналах учета (журнальный учет), в карточках учета (карточный учет) или с использованием средств вычислительной техники (автоматизированный учет).

В журналах (карточках) учета отражаются данные о движении документов с момента их получения или подготовки до завершения исполнения и подшивки в дело, отправки адресатам или уничтожения.

Учет подготовленных документов, отправка исходящих документов

Документы, отправляемые органами внутренних дел, передаются почтовой связью, электросвязью и с использованием ведомственной магистральной сети передачи данных (МСПД).

Обработка документов для отправки почтовой связью осуществляется подразделениями делопроизводства и режима органов внутренних дел в соответствии с Правилами оказания услуг почтовой связи, утвержденными постановлением Правительства РФ от 15 апреля 2005г. № 221.

С помощью средств электросвязи осуществляется передача информации в виде телеграмм, телетайпограмм, факсограмм, телефонограмм, электронных сообщений.

Запрещается передача с помощью средств электросвязи документов, имеющих грифы секретности, и пометку «Для служебного пользования».

Документы, подлежащие отправке, обрабатываются и отправляются в день их подписания или не позднее следующего рабочего дня. Учет подготовленных и отправляемых (исходящих) документов после их подписания руководителем органа внутренних дел или уполномоченным на это должностным лицом осуществляется в журнале учета подготовленных несекретных документов или в карточке учета подготовленных несекретных документов.

Неправильно оформленные документы возвращаются сотрудниками подразделения делопроизводства и режима исполнителям для доработки.

Документы могут направляться адресатам за своими регистрационными номерами без сопроводительных писем, если предназначение этих документов не требует пояснения.

Каждый исходящий служебный документ, как правило, должен иметь второй экземпляр, который заверяется сотрудником подразделения делопроизводства и режима. Второй экземпляр списывается руководителем соответствующего структурного подразделения и подшивается в дело вместе с исполненным документом. Если второй экземпляр исходящего документа требуется для работы, он выдается исполнителю под расписку в журнале (карточке) учета подготовленных несекретных документов.

При печатании 5 и более экземпляров документа исполнитель документа на обороте последнего листа экземпляра документа, остающегося в деле, или на отдельном листе составляет указатель рассылки.

В тех случаях, когда к исходящему служебному документу прилагается служебный документ, имеющий входящий, инвентарный или другой номер, в соответствующем журнале учета указываются наименование адресата, которому отправляется этот документ, а также номер и дата исходящего служебного документа, с которым он отправлен.

При необходимости отправки входящих (инвентарных) служебных документов в другие органы внутренних дел они могут пересылаться за присвоенными им входящими (инвентарными) номерами. В соответствующих журналах (карточках) учета указываются, кому отправляется служебный документ, порядковый номер реестра (по разносной книге) и дата отправки.

Если поставленные в документе вопросы не требуют аргументированных разъяснений или подготовки какого-либо документа, разрешается давать ответы непосредственно на поступивших служебных документах с последующим возвращением их за входящими номерами.

Текст ответа не должен осуществляться с наложением на текст документа, его реквизитов и затруднять его прочтение.

Прием, обработка, распределение и исполнение поступающих документов

Доставка документов в органы внутренних дел осуществляется, как правило, средствами почтовой и фельдъегерской связи, электросвязи, курьерами.

С помощью почтовой связи в органы внутренних дел доставляется письменная корреспонденция в виде простых и регистрируемых писем, почтовых карточек, бандеролей, мелких пакетов, а также печатные издания.

Прием документов включает: проверку правильности его доставки; проверку сохранности упаковки (пакета, конверта); вскрытие конвертов; проверку правильности вложений.

Документы, поступающие в органы внутренних дел на бумажных носителях, проходят первичную обработку, предварительное рассмотрение, регистрацию, рассмотрение руководством и передаются исполнителям.

Вся поступающая корреспонденция в рабочее время принимается сотрудниками подразделения делопроизводства и режима. Сотрудник, принимающий корреспонденцию, проверяет правильность адресования пакетов, сверяет номера на пакетах с номерами, указанными в реестре (разносной книге, расписке), после чего расписывается (с указанием своей фамилии) в ее получении в реестре (разносной книге, расписке), указывает прописью количество принятых пакетов, дату и время их приема, заверяет свою подпись соответствующей печатью или штампом органа внутренних дел.

В нерабочее время корреспонденция принимается дежурным по органу внутренних дел, который регистрирует поступившие пакеты в журнале учета пакетов и, не вскрывая, передает их под расписку в этом журнале в подразделение делопроизводства и режима. О получении срочных пакетов дежурный незамедлительно докладывает руководителю органа внутренних дел либо ответственному от руководства органа внутренних дел.

Руководитель органа внутренних дел или ответственный от руководства органа внутренних дел вскрывает пакет и после рассмотрения с резолюцией возвращает дежурному. В случае необходимости немедленного размножения либо доведения содержания несекретного документа, находящегося в пакете, до других лиц это может быть поручено дежурному, с отражением указания в резолюции. Дежурный составляет справку о том, сколько сделано копий, когда и кому они вручены, а также когда и кому устно доведено содержание документа; подписывает справку с указанием даты и времени, приобщает ее к документу. Лица, получающие копию, обязаны расписаться в справке с указанием даты и времени. Дежурный передает документ вместе со справкой и пакетом в подразделение делопроизводства и режима не позднее начала следующего рабочего дня.

Поступившая в подразделение делопроизводства и режима корреспонденция вскрывается, за исключением конвертов с пометкой «Лично». Такие пакеты регистрируются без вскрытия и передаются адресату или уполномоченному на то сотруднику. Сотрудник, вскрывающий пакет, должен убедиться в полном изъятии из него корреспонденции. При вскрытии конвертов проверяется правильность адресования и оформления, комплектность и целостность документов и приложений к ним, сверяются номера документов с номерами, указанными на пакете.

При поступлении поврежденного документа на оборотной стороне его последнего листа в правом нижнем углу ставится отметка «Документ получен в поврежденном виде».

Конверты от поступившей корреспонденции после проверки уничтожаются, за исключением случаев, когда только по ним можно установить адрес отправителя или, когда дата почтового штемпеля имеет значение в качестве доказательства времени отправки и получения документа.

Ошибочно направленные документы возвращаются отправителю или по согласованию с ним пересылаются по назначению в новых пакетах (упаковках) за регистрационными номерами отправителя (без взятия на основной учет подразделением делопроизводства и режима) с приложением части пакета отправителя, содержащей все надлежащие пометки.

Поступившие документы учитываются и распределяются на регистрируемые и нерегистрируемые. Каждый орган внутренних дел разрабатывает собственный перечень нерегистрируемых документов.

После вскрытия пакета документы регистрируются в журнале или в карточке учета входящих несекретных документов либо в других учетных документах. При наличии в пакете нескольких документов каждый из них регистрируется за отдельным номером.

При регистрации входящего документа на его первом листе ставится штамп с указанием наименования органа внутренних дел, получившего документ, регистрационного (входящего) номера, даты регистрации, количества листов основного документа и приложений к нему. На первых листах приложений ставится штамп «К вх. N \_\_\_\_\_» с указанием года регистрации.

Документы, адресованные руководству органа внутренних дел, а также без указания конкретного лица или структурного подразделения предварительно рассматриваются в подразделении делопроизводства и режима, а затем направляются непосредственно руководству или в структурное подразделение.

Предварительное рассмотрение документов проводится с целью распределения поступивших документов на потоки: требующие обязательного рассмотрения руководством; направляемые непосредственно в структурные подразделения и ответственным исполнителям.

Предварительное рассмотрение осуществляется, исходя из оценки их содержания, на основании установленного в органе внутренних дел распределения служебных обязанностей.

Без предварительного рассмотрения передаются по назначению документы, адресованные непосредственно структурным подразделениям органа внутренних дел или конкретным должностным лицам.

После регистрации корреспонденция докладывается, как правило, в день поступления руководителю органа внутренних дел или передается сотруднику, которому она адресована.

При рассмотрении документов руководитель органа внутренних дел определяет в резолюции исполнителя (структурное подразделение или должностное лицо) и сроки исполнения. Резолюция должна быть лаконичной, содержать порядок и характер исполнения документа, а также фамилии и инициалы исполнителей, подпись руководителя и дату. Резолюция пишется на документе, отдельном листе, либо на специальном бланке.

После доклада корреспонденции руководству органа внутренних дел резолюция переносится в соответствующую графу журнала (карточки) учета входящих несекретных документов либо вносится в систему электронного документооборота.

Документы, которые исполняются несколькими структурными подразделениями, передаются им поочередно или одновременно в копиях. Подлинник передается ответственному исполнителю.

Направление документов на исполнение производится в день их регистрации, а срочных и оперативных документов - незамедлительно.

Служебные документы передаются исполнителю под расписку в журнале (карточке) учета входящих несекретных документов с проставлением даты получения. Передача служебных документов из одного структурного подразделения органа внутренних дел в другое осуществляется через подразделение делопроизводства и режима.

Исполнение документа предусматривает сбор и обработку необходимой информации, подготовку, при необходимости, проекта документа, его оформление, согласование, представление на подписание (утверждение) руководителю органа внутренних дел или структурного подразделения органа внутренних дел.

Исполнитель несет персональную ответственность за полноту и достоверность информации, использованной при подготовке документа, нарушение установленных сроков исполнения документов без объективных причин.

При оперативном решении вопросов без составления дополнительных документов исполнителем делаются отметки на документе: о дате поступления (если образовался интервал времени между поступлением документа и его доставкой исполнителю), о датах и ходе промежуточного исполнения (запрос сведений, телефонные переговоры и другое), о дате и результатах окончательного исполнения.

Все отметки размещаются на свободных от текста местах.

При возвращении документа из структурного подразделения в подразделение делопроизводства и режима (после исполнения или ознакомления) его повторная регистрация не производится, а делается отметка в учетных формах о движении документа.

Составление номенклатуры дел

В целях правильного формирования дел, систематизированного хранения особой важности, совершенно секретных, секретных и несекретных документов и оперативного их поиска составляется номенклатура особой важности, совершенно секретных, секретных и несекретных дел.

Номенклатура дел - систематизированный перечень заголовков дел, заводимых в органе внутренних дел с указанием сроков их хранения, оформленный в установленном порядке. Номенклатура дел является классификационным справочником и используется при построении информационно-поисковой системы и является основным учетным документом дел текущего года.

Номенклатура дел является основным регистрационным документом дел текущего года и основанием их регистрации после окончания ведения в журнале учета законченных производством дел. Порядковые номера дел по номенклатуре дел являются номерами дел текущего года.

Номенклатура дел составляется на основе изучения состава, содержания и количества документов, образующихся в процессе деятельности органа внутренних дел.

При составлении номенклатуры дел следует руководствоваться положением об органе внутренних дел, положениями о его структурных подразделениях, штатным расписанием, планами и отчетами о работе, перечнями документов с указанием сроков их хранения, номенклатурами дел за предшествующие годы.

В каждом органе внутренних дел составляется сводная номенклатура дел. В структурных и подчиненных (подведомственных) подразделениях, имеющих самостоятельное делопроизводство, в зависимости от объема документооборота и места дислокации допускается составление отдельных номенклатур дел.

Номенклатура дел на предстоящий календарный год составляется в IV квартале текущего года подразделением делопроизводства и режима совместно с руководителями других структурных подразделений, а также руководителем подразделения специальных фондов, подписывается руководителем подразделения делопроизводства и режима, согласовывается с подразделением специальных фондов, после чего утверждается руководителем органа внутренних дел и вводится в действие с 1 января следующего календарного года.

Формирование дел

Формированием дел называется группировка исполненных документов в дела в соответствии с номенклатурой дел.

Номенклатурные дела формируются в органах внутренних дел:

-  при централизованном ведении делопроизводства - подразделением делопроизводства и режима;

-при децентрализованном ведении делопроизводства как структурными подразделениями органа внутренних дел (лицами, ответственными за ведение дел), так и подразделением делопроизводства и режима.

Ведение и хранение дел непосредственно сотрудниками структурных подразделений органа внутренних дел допускается с письменного разрешения руководителя органа внутренних дел и по согласованию с руководителем подразделения делопроизводства и режима.

Формирование дел осуществляется в соответствии со следующими общими правилами:

- к делам приобщаются только исполненные документы в соответствии с заголовками дел по номенклатуре дел;

- в дело группируются документы одного календарного года (исключение составляют переходящие дела и документы, переходящие сроком исполнения на последующий год);

- документы постоянного и временного сроков хранения группируются в отдельные дела;

- каждый документ, помещенный в дело, должен быть оформлен в соответствии с требованиями государственных стандартов и нормативных правовых актов МВД России;

-в дело включается по одному экземпляру каждого документа;

- в делах оформляются внутренние описи документов, находящихся в деле;

- по объему дело не должно превышать 250 листов, при толщине не более 40мм. При наличии в деле нескольких томов индекс и заголовок дела проставляется на каждом томе с добавлением «т.1», «т.2» и далее.

При приеме исполненных документов проверяется правильность их оформления (наличие подписей, виз, отметок об исполнении, дат, номеров и заверительных надписей), правильность рассылки, направления документов в дела и наличие фамилий исполнителей документов, а также соответствие грифа ограничения доступа документов грифу секретности дела, количество листов и наличие указанных в документе приложений.

Неисполненные, подлежащие возврату, неправильно оформленные документы на подшивку не принимаются.

Несекретные документы подшиваются с совершенно секретными и секретными, если они соответствуют заголовку номенклатурного дела.

## Выбор и обоснование методов защиты систем электронного документооборота

### Аутентификация

Процесс доступа пользователя в систему в большинстве случаев состоит из двух частей – идентификации и аутентификации. Идентификация – это предъявление пользователем какого-то уникального, присущего только ему признака-идентификатора. Это может быть пароль, какая-то биометрическая информация, например отпечаток пальца, персональный электронный ключ или смарт-карта и т.д. Аутентификация – это процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу.

Эти процедуры неразрывно связаны между собой, поскольку способ проверки определяет, каким образом и что пользователь должен предъявить системе, чтобы получить доступ.

Подсистема идентификации и аутентификации пользователей — важнейший компонент системы информационной безопасности, и ее значение трудно переоценить. Подсистема подтверждает личность пользователя информационной системы и поэтому должна быть надежной и адекватной, то есть исключать все ошибки в предоставлении доступа. Существующие методы аутентификации различны по степени надежности, и, как правило, с усилением защиты резко возрастает цена систем, что требует при выборе средств аутентификации анализа рисков и оценки экономической целесообразности применения тех или иных мер защиты. Однако в последнее время «соотношение сил» в области эффективности применяемых методов аутентификации меняется.

Средства аутентификации можно разделить на три группы («фактора») в соответствии с применяемыми принципами: принцип «что вы знаете» («you know»), лежащий в основе методов аутентификации по паролю; принцип «что вы имеете» («you have»), когда аутентификация осуществляется с помощью магнитных карт, токенов и других устройств; и принцип «кто вы есть» («you are»), использующий персональные свойства пользователя (отпечаток пальца, структуру сетчатки глаза и т. д.). Системы строгой аутентификации используют 2 и более факторов при аутентификации пользователей.

На сегодняшний день средства аутентификации первой группы являются самыми экономичными по стоимости, но одновременно и наименее надежными.

Метод аутентификации по паролю является наиболее традиционным и распространенным. Однако парольная аутентификация имеет настолько много недостатков, что в ситуациях, где неверные результаты аутентификации используется в паре с каким-то другим методом. Основные недостатки парольной аутентификации таковы:

* + достаточно часто пользователи применяют легко предсказуемые пароли, например: – пароль эквивалентен имени пользователя или имени пользователя в обратной последовательности, или какой-либо другой производной от имени пользователя; – пароль является словом или фразой какого-либо языка – пароль может быть подобран путем словарной атаки, т. е. перебора в качестве пароля всех слов по словарю; программы, выполняющие подобные атаки, существуют в Интернете в великом множестве;
  + существуют различные программы подбора паролей для наиболее популярных приложений и операционных систем.
  + пароль может быть перехвачен или подсмотрен при его вводе либо получен путем применения насилия к его владельцу.

Последствия особенно опасны в системах, где используется принцип «единого входа» (single sign-on), когда сотрудник применяет один пароль для аутентификации и работы со многими корпоративными приложениями и источниками информации. Часто, не осознавая важности аутентификации, сотрудники практикуют передачу личного пароля коллегам. Здесь стоит отметить, что процедура аутентификации тесно связана с другими процессами в системе информационной безопасности, например с мониторингом действий в системе, и при расследовании инцидента, не имея строгой идентификации пользователя, нередко очень тяжело установить причину инцидента.

Системы строгой аутентификации, построенные на факторе «you know» и «you have», предоставляют больше возможностей для усиления защиты. Например, работу токенов, которые генерируют одноразовые пароли, не имея соединения с защищаемой системой, очень сложно подделать, а сам пароль не может быть повторно использован. Примерами могут служить устройства RSA SecureID и Vasco Digipass. Наиболее интересно применение этих устройств в таких областях, как электронная коммерция, включая интернет-банкинг, или для организации защиты ключевых с точки зрения безопасности пользователей (администраторов информационной системы и руководителей). Этими устройствами можно пользоваться для проведения аутентификации при удаленном доступе с рабочего места, имеющего низкий уровень доверия, например при работе в интернет-кафе. Но такой способ аутентификации также не лишен недостатков — токен, например, можно передать вместе с ПИН другому пользователю.

С этой точки зрения более строгую аутентификацию обеспечивают средства, основанные на биометрических методах, интерес к которым сейчас активно растет, что связано не в последнюю очередь с постепенным снижением их стоимости.

Биометрические системы идентификации, доступные в настоящее время или находящиеся в стадии разработки, включают системы доступа по отпечатку пальца, запаху, ДНК, форме уха, геометрии лица, температуре кожи лица, клавиатурному почерку, отпечатку ладони, рисунку вен ладони, структуре сетчатки глаза, рисунку радужной оболочки глаза, подписи и голосу.

### Межсетевое экранирование

Важное место в списке средств обеспечения информационной безопасности от внешних атак занимают межсетевые экраны (часто называемые брандмауэрами, или, по-английски, firewall). Согласно «Руководящему документу. Межсетевые экраны» Гостехкомиссии при Президенте РФ «межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т. е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе». К сожалению, такое определение имеет чересчур общий характер и подразумевает слишком расширенное толкование.

В обиходе межсетевыми экранами (МЭ) называют средства защиты, устанавливаемые между общедоступной (такой, как Internet) и внутренней сетью. Межсетевой экран выполняет двойную функцию. Во-первых, он призван ограничить доступ во внутреннюю сеть со стороны общедоступной сети за счет применения фильтров и средств аутентификации, чтобы злоумышленники не могли получить несанкционированный доступ к информации или нарушить нормальную работу сетевой инфраструктуры. Во-вторых, МЭ служит для контроля и регулирования доступа пользователей внутренней сети к ресурсам общедоступной сети, когда те представляют угрозу безопасности или отвлекают сотрудников от работы (порнографические, игровые, спортивные серверы).

Часто сетевые экраны устанавливают и внутри корпоративных сетей, в целях ограничения доступа пользователей к особо важным ресурсам сети, например к серверам, содержащим финансовую информацию или сведения, относящиеся к коммерческой тайне. Существуют также персональные межсетевые экраны, призванные регулировать доступ к отдельным компьютерам и устанавливаемые на эти компьютеры.

Межсетевые экраны по понятным причинам используются для сетей TCP/IP и классифицируются в соответствии с уровнем эталонной модели взаимодействия открытых систем (сетевой моделью) OSI. Однако такая классификация, в силу ряда обстоятельств носит достаточно условный характер. Во-первых, сетевая модель сетей TCP/IP предусматривает только 5 уровней (физический, интерфейсный, сетевой, транспортный и прикладной), в то время как модель OSI — 7 уровней (физический, канальный, сетевой, транспортный, сеансовый, презентационный и прикладной). Поэтому установить однозначное соответствие между этими моделями далеко не всегда возможно. Во-вторых, большинство выпускаемых межсетевых экранов обеспечивают работу сразу на нескольких уровнях иерархии OSI. В-третьих, некоторые экраны функционируют в режиме, который трудно соотнести с каким-то строго определенным уровнем иерархии.

Существует также понятие «межсетевой экран экспертного уровня». Такие МЭ обычно базируются на посредниках прикладного уровня или инспекторах состояния, но обязательно комплектуются шлюзами сеансового уровня и сетевыми фильтрами. К МЭ экспертного класса относятся почти все имеющиеся на рынке коммерческие брандмауэры.

Межсетевые экраны могут опираться на один из двух взаимоисключающих принципов обработки поступающих пакетов данных. Первый принцип гласит: «Что явно не запрещено, то разрешено». Т. е. если МЭ получил пакет, не подпадающий не под одно из принятых ограничений или не идентифицированный правилами обработки, то он передается далее. Противоположный принцип — «Что явно не разрешено, то запрещено» — гарантирует гораздо большую защищенность, но оборачивается дополнительной нагрузкой на администратора. В этом случае внутренняя сеть изначально полностью недоступна, и администратор вручную устанавливает разрешенные при обмене данными с общедоступной сетью сетевые адреса, протоколы, службы и операции.

Правила обработки информации во многих межсетевых экранах экспертного класса могут иметь многоуровневую иерархическую структуру. Например, они могут позволять задать такую схему: «Все компьютеры локальной сети недоступны извне, за исключением доступа к серверу A по протоколу ftp и к серверу B по протоколу telnet, однако при этом запрещен доступ к серверу A с операцией PUT сервиса ftp».

Межсетевые экраны могут выполнять над поступающими пакетами данных одну из двух операций: пропустить пакет далее (allow) или отбросить пакет (deny). Некоторые МЭ имеют еще одну операцию — reject, при которой пакет отбрасывается, но отправителю сообщается по протоколу ICMP о недоступности сервиса на компьютере-получателе информации. В противовес этому при операции deny отправитель не информируется о недоступности сервиса, что является более безопасным.

Итак, брандмауэр — это система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения информации из одной части в другую. Брандмауэры представляют собой целый класс систем, порой сопоставимых по сложности с операционной системой. Классифицировать их можно по исполнению: программные, аппаратные и смешанного типа (аппаратно-программного); по компонентной модели: локальные (работающие на одном хосте) и распределенные (distributed firewall). Однако самой «полезной» является классификация с точки зрения уровня, на котором функционируют брандмауэры: пакетный уровень, прикладной, уровень соединения.

Разбивка на уровни является условной, что подразумевает возможность работы отдельно взятого брандмауэра более чем на одном уровне одновременно. Можно сказать, что практически все современные брандмауэры функционируют сразу на нескольких уровнях, стремясь расширить функциональность и максимально использовать преимущества работы по той или иной схеме. Такая технология получила название Stateful Inspection, а брандмауэры, работающие по смешанной схеме, называются Stateful Inspection Firewall.

Идеальный персональный брандмауэр должен выполнять шесть функций:

* Блокировка внешних атак. В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр.
* Блокировка утечки информации. Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть.
* Контроль приложений. Неизбежное наличие открытых портов является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через порты — контроль приложений, запрашивающих разрешение на доступ. Кроме банальной проверки по имени файла, весьма желательна проверка аутентичности приложения.
* Поддержка зональной защиты Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как правило, потенциально опасных) технологий. В то же время уровень доверия к Интернет-контенту значительно ниже, а значит, необходим дифференцируемый подход к анализу опасности того или иного содержания.
* Протоколирование и предупреждение. Брандмауэр должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются.
* Максимально прозрачная работа Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения.

В общем случае методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети реализует следующие основные функции.

***1. Многоуровневая фильтрация сетевого трафика***

Фильтрация обычно происходит на четырех уровнях OSI:

* Канальном (Ethernet).
* Сетевом (IP).
* Транспортном (TCP, UDP).
* Прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация сетевого трафика является основной функцией систем Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику в выделенном сегменте IP-сети, то есть, настроив соответствующим образом Firewall, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящимся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Можно провести аналогию с администратором локальной ОС, который для осуществления политики безопасности в системе назначает необходимым образом соответствующие отношения между субъектами (пользователями) и объектами системы (файлами, например), что позволяет разграничить доступ субъектов системы к ее объектам в соответствии с заданными администратором правами доступа. Те же рассуждения применимы к Firewall-фильтрации: в качестве субъектов взаимодействия будут выступать IP-адреса хостов пользователей, а в качестве объектов, доступ к которым необходимо разграничить, - IP-адреса хостов, используемые транспортные протоколы и службы предоставления удаленного доступа.

***2. Proxy-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте***

Proxy-схема позволяет, во-первых, при доступе к защищенному Firewall сегменту сети осуществить на нем дополнительную идентификацию и аутентификацию удаленного пользователя и, во-вторых, является основой для создания приватных сетей с виртуальными IP-адресами. Смысл proxy-схемы заключается в создании соединения с конечным адресатом через промежуточный proxy-сервер (в переводе с англ. "proxy" - полномочный) на хосте Firewall.

***3. Создание приватных сетей с "виртуальными" IP-адресами***

Если администратор безопасности сети считает целесообразным скрыть истинную топологию своей внутренней IP-сети, то ему можно порекомендовать использовать системы Firewall для создания виртуальных сетей с применением технологии NAT (Network Address Translation). Для адресации во внешнюю сеть через Firewall необходимо либо использовать на хосте Firewall описанные выше proxy-серверы, либо применять только специальные системы маршрутизации (через которые и возможна внешняя адресация). Это происходит из-за того, что используемый во внутренней приватной сети "виртуальный" IP-адрес, очевидно, непригоден для внешней адресации, то есть адресации к абонентам, находящимся за ее пределами. Поэтому proxy-сервер должен осуществлять связь с абонентами из внешней сети со своего настоящего IP-адреса.

Итак, любое устройство, реализующее хотя бы одну из этих функций Firewall-методики, и является Firewall-устройством. Например, ничто не мешает использовать в качестве Firewall-хоста компьютер с обычной ОС FreeBSD или Linux, у которой соответствующим образом нужно скомпилировать ядро ОС. Firewall такого типа будет обеспечивать только многоуровневую фильтрацию IP-трафика. Другое дело - предлагаемые на рынке мощные Firewall-комплексы, созданные на базе ЭВМ или мини-ЭВМ, обычно реализуют все функции Firewall-методики и являются полнофункциональными системами Firewall.

## Выбор и обоснование программных и аппаратных средств для обеспечения защиты систем электронного документооборота

### Выбор персонального брандмауэра

Для обеспечения защиты от несанкционированного доступа к компьютерам пользователей систем электронного документооборота необходимо применить брандмауэр.

Программные брандмауэры в сегментах сети и ее ядре уже используются в виде встроенных в машрутизаторы функций распределения трафика.

Поэтому необходимо выбрать персональный брандмауэр, который бы программно защищал каждый персональный компьютер локальной вычислительной сети, на основе которой функционирует система электронного документооборота.

На сегодняшний день имеется немало известных, зарекомендовавших себя продуктов, среди которых можно найти и бесплатные (а большинство платных имеют 30-дневный бесплатный период). Следует заметить, что в настоящее время уже в сильной мере проявилась тенденция, связанная с разработкой программ для комплексной защиты компьютера, то есть таких, которые выполняют и обычные функции файрволла, блокируя несанкционированный доступ к вашему компьютеру извне, и защищают от спама, предупреждают о подозрительных сайтах, ведут борьбу с вирусами и троянами и т. п. Именно такой пакет комплексной защиты, выпущенный одним производителем, является оптимальным выбором.

Конечно же, самым главным параметром является надёжность файрволла, степень предоставления защиты и способность отражать различные атаки и угрозы. Но этот параметр не является единственным, на который стоит обращать внимание. Немаловажно также удобство пользования файрволлом, простота настройки параметров, требования к производительности и степень загрузки ресурсов компьютера во время работы.

В рамках проекта по тестированию файрволлов[[1]](#footnote-1) было проведено их испытания и сравнение. В таблице 3.1 список продуктов, прошедших полный набор из 148 тестов и их рейтинг на сегодняшний момент.

Таблица 3.1

Сравнение файрволлов

|  |  |  |  |
| --- | --- | --- | --- |
| **Продукт** | **Рейтинг** | **Достиг ступени теста** | **Уровень защиты** |
| Outpost Security Suite FREE 7.0.4.3418.520.1245.401 Бесплатный | 100% | 10+ | Отличный |
| PC Tools Internet Security 2011 8.0.0.623 | 99% | 10+ | Отличный |
| Online Solutions Security Suite 1.5.14905.0 | 99% | 10+ | Отличный |
| Outpost Security Suite Pro 7.0.1.3376.514.1234.401 | 97% | 10+ | Отличный |
| Kaspersky Internet Security 2011 11.0.1.400 | 92% | 10+ | Отличный |
| Malware Defender 2.6.0 | 90% | 10 | Очень хороший |
| Privatefirewall 7.0.21.1 Бесплатный | 89% | 9 | Очень хороший |
| BitDefender Internet Security 2011 14.0.24.330 | 84% | 10+ | Очень хороший |
| ZoneAlarm Extreme Security 9.1.008.000 | 59% | 7 | Плохой |
| Rising Internet Security 2010 22.33.00.01 | 55% | 8 | Плохой |
| Norton Internet Security 2011 18.1.0.37 | 40% | 6 | Плохой |
| Jetico Personal Firewall 2.1.0.7.2412 | 28% | 4 | Никакой |
| Dr.Web Security Space Pro 6.0.2.07290 | 14% | 3 | Никакой |
| CA Internet Security Suite Plus 2010 6.0.0.285 | 12% | 3 | Никакой |
| F-Secure Internet Security 2010 10.00.246 | 9% | 2 | Никакой |
| Trend Micro Internet Security Pro 2010 17.50.1647.0000 | 9% | 2 | Никакой |
| FortKnox Personal Firewall 6.0.205.0 | 7 % | 2 | Никакой |
| ZoneAlarm Firewall 9.2.076.000 Бесплатный | 7 % | 2 | Никакой |
| ESET Smart Security 4.2.64.12 | 6 % | 2 | Никакой |
| avast! Internet Security 5.0.418.0 | 3 % | 1 | Никакой |
| Avira Premium Security Suite 10.0.0.542 | 3 % | 1 | Никакой |

Как видим, на вершине данного рейтинга находится Outpost Security Suite российской компании Agnitum - один из наиболее известных файрволлов. Outpost Security Suite - комплексное решение, включающее защиту от вирусов, троянов, шпионских программ, контроль приложений, защиту от спама, блокирование нежелательной рекламы, защиту от посещения нежелательных сайтов и т. п. Одно из самых лучших и надёжных решений. Есть как несколько урезанная в возможностях настроек бесплатная, так и платная версии.

Следовательно, для использования в системе электронного документооборота выберем именно данный брандмауэр.

К основным возможностям данного брандмауэра относится:

* Защита системы и приложений

В Outpost 7 реализованы два новых инструмента, которые укрепляют защиту и оберегают целостность системы, предоставляя инструменты для контроля взаимодействия приложений и системы и распределения ресурсов между ними.

* Защита файлов и папок
* Превентивная защита

Outpost контролирует поведение и взаимодействие приложений, закрывая бреши в системе защиты. Анализируя угрозы и отображая своевременные уведомления, многогранная «Проактивная защита» Outpost 7 блокирует все виды изощренных методов взлома, используемых для кражи данных, останавливает новейшие атаки и защищает компьютер от несанкционированных действий, делая ПК неподвластным таким угрозам безопасности, как компьютеры-зомби и руткиты.

* Внутренняя защита

Современные вредоносные программы часто пытаются деактивировать защиту компьютера, чтобы облегчить процесс его заражения и захвата. Бдительность и неусыпный контроль состояния всех своих компонентов, осуществляемый Outpost 7, делает невозможным выключение защиты кем-либо кроме авторизованного пользователя программы.

* Сетевая безопасность и целостность
* Контроль доступа приложений

Брандмауэр контролирует список программ, которым разрешен доступ в Интернет, заранее защищая ваш компьютер от новейших угроз и попыток вредоносных программ передать данные на сервер их авторов.

* Оптимизированный брандмауэр
* Безопасность соединений

Двусторонний брандмауэр контролирует входящие и исходящие соединения вашего компьютера и предотвращает несанкционированные попытки доступа из локальной и внешней (Интернет) сети. Брандмауэр скрывает порты, делая присутствие компьютера в сети невидимым. Модуль Ethernet-безопасности защищает ваши локальные соединения и предотвращает вредительство в локальной сети, контролируя передачу данных. Это снижает вероятность того, что данные, передающиеся, например, в чат-окнах или сессиях браузера, будут доставлены по неверному адресу или перехвачены.

* Всесторонняя защита

Outpost защищает все типы соединений (Ethernet, WiFi, DSL, кабельные, сотовые и соединения dial-up), автоматически применяя необходимые настройки безопасности при подключении компьютера к новому провайдеру. Соединения Wi-Fi дополнительно защищены от прослушивания и нелегального проникновения.

* Защита от вторжений
* Круговая антивирусная защита

Универсальный модуль «Антивирус + Антишпион» следит за тем, чтобы в ваш компьютер не проникли вирусы, руткиты и другие образцы вредоносного ПО. Монитор доступа в фоновом режиме проверяет уязвимые места компьютера на наличие вредоносных объектов, а антивирусный сканер позволяет провести дополнительную проверку на жестком диске, в сетевых папках, на DVD и внешних устройствах хранения данных.

* Проверка USB-устройств и вложений электронной почты

Съемные USB-устройства, автоматически проверяются на наличие угроз при подключении их к компьютеру. Почтовые вложения проверяются и автоматически дезинфицируются в режиме реального времени в момент отправки или получения. Вы также можете поместить любой подозрительный файл в карантин для последующей обработки. Эти функции исключают возможность заражения вашего ПК из-за неосторожности других, также как и ваша собственная почта не будет представлять опасность для ваших корреспондентов.

* Расширенный эвристический анализатор

Эвристический анализатор мониторит поведение процессов, которые запускаются одновременно с системой Windows, а антивирусный модуль Outpost проверяет подозрительные объекты на предмет наличия потенциальных угроз и использования уязвимостей системы. Это увеличивает степень защиты от запакованных эксплойтов и вредоносных исполняемых файлов, которые не могут быть обнаружены традиционными сигнатурными методами.

### Выбор дополнительного средства аутентификации

Как уже было показано выше, обычная парольная защита в силу своих особенностей и психологии людей не может быть признана достаточно надежной. Отсюда вытекает необходимость применения дополнительных средств аутентификации пользователей системы электронного документооборота.

Таким средством должны стать электронные ключи eToken – персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП). Модельный ряд eToken представлен USB-ключами, смарт-картами, комбинированными устройствами и автономными генераторами одноразовых паролей (OTP).

Используя электронные ключи eToken, можно решить следующие задачи:

* усовершенствовать процесс аутентификации (двухфакторная аутентификация) на локальном компьютере и в корпоративной сети, а также защищенный доступ к бизнес-приложениям;
* зашифровать данные на серверах, ноутбуках и рабочих станциях;
* обеспечить защиту персональных данных;
* защитить электронную почту и взаимодействие с коллегами в системах электронного документооборота;
* обезопасить себя от кражи паролей к онлайн-сервисам.

Для использования предлагается продукт компании "Алладин" "eToken для Microsoft Windows 2000/XP/2003". Данное решение выполняет следующие функции:

* Вход в компьютер и сеть с использованием eToken и цифровых сертификатов
* Решение проблемы "слабых" паролей
* Решение проблемы хранения ключей ЭЦП и шифрования
* Безопасное администрирование
* Интеграция в инфраструктуру открытых ключей

"eToken для Microsoft Windows 2000/XP/2003"[[2]](#footnote-2) обеспечивает строгую двухфакторную аутентификацию пользователей при входе в сеть на основе цифровых сертификатов стандарта Х.509.

eToken используется для генерации ключевых пар RSA (открытый и закрытый ключи), выполнения криптографических операций с закрытым ключом в доверенной среде (например, формирование ЭЦП), а также надёжного хранения цифровых сертификатов и ключевой информации.

Для системных администраторов и администраторов безопасности особый интерес представляют следующие возможности:

* полный отказ от парольной аутентификации в пользу строгой двухфакторной аутентификации;
* защищённое удалённое администрирование по протоколу RDP серверов и рабочих станций с аутентификацией по eToken;
* настройка сервера маршрутизации и удаленного доступа для подключения клиентов только по защищённым каналам с обязательной аутентификацией по eToken.

## Выводы:

В качестве методов повышения защищенности были выбраны использование персональных брандмауэров на компьютерах пользователей СЭД, а также аппаратные решения для повышения достоверности аутентификации и доступа к системе.

# Заключение

Итак, в настоящей работе рассмотрены мероприятия, которые необходимо осуществить в ОВД для повышения защищенности систем электронного документооборота.

В первой главе дипломной работы рассмотрены определение, функции и задачи систем электронного документооборота, а также аспекты нормативно-правового регулирования обеспечения информационной безопасности СЭД как части информационной системы ОВД,

Во второй части дипломной работы рассмотрены основные угрозы информационной безопасности СЭД, а также методы обеспечения безопасности.

В третьей части приведены основные решения по организационно-административным мерам защиты информации, рассмотрены и выбраны методы защиты от несанкционированного доступа, а также произведен выбор программных и аппаратных решений.

Обработка информации в СЭД ОВД ведется именно с применением технических средств, размещаемых в локальной вычислительной сети. В работе основными мерами по СЭД указаны:

* 1. Разграничение доступа к ресурсам;
  2. Дополнительная двухфакторная аутентификация (с использованием eToken);
  3. Использование персональных брандмауэров (Outpost Security Suite Free).

Очевидно, что только при комплексном подходе к обеспечению информационной безопасности предприятия значительно понижается вероятность несанкционированного доступа к информации, обрабатываемой в СЭД. Однако обеспечение безопасности данных – это процесс прежде всего, и поэтому в этой области работа должна быть постоянной и непрерывной.

# Список использованной литературы

1. ГОСТ Р 51141-98, «Делопроизводство и архивное дело. Термины и определения (взамен ГОСТ 16487-83)».
2. ГОСТ Р 6.30-97, «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».
3. Лапонина О. Р., Межсетевое экранирование, Бином,  2007 г.-354с.
4. Лебедь С. В., Межсетевое экранирование: Теория и практика защиты внешнего периметра, Издательство Московского технического университета им. Баумана, 2002 г, 304 с.
5. Лопатин В.Н. Информационная безопасность России. Человек. Общество. Государство. Санкт-Петербургский университет МВД РФ.- С-П.: Фонд «Университет».-2000.- 428 с.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов.- М.: Горячая линия-Телеком. -2004.-280 с.
7. Олифер В.Г., Олифер Н.А. ,Компьютерные сети. Принципы, технологии, протоколы, 2-е изд, СПб, Питер-пресс, 2002 год, 465 с.
8. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебное пособие-М.: Радио и связь, 2001г.-368с.
9. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности, СпБ, Питер, 2008 г.- 320 с.
10. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998 г. - 320 с.
11. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации(под редакцией Ковтанюка) К.: Издательство Юниор, 2003г.-504 стр.
12. Ярочкин В.И. Информационная безопасность. Учебное пособие,. — М.: Междунар. отношения, 2000. — 400 с.: ил.

1. <http://www.matousec.com/> [↑](#footnote-ref-1)
2. http://www.aladdin-rd.ru/catalog/etoken\_products/archive/win2000/ [↑](#footnote-ref-2)