Содержание

Введение

1. Теоретические основы безопасности и защиты информации в компьютерных сетях

1.1 Сущность проблемы и задачи защиты в компьютерных сетях

.2 Угрозы, атаки и каналы утечки информации

.3 Методы обеспечения безопасности сетей

.4 Правовые аспекты защиты информации

. Методы и средства защиты информации в сетях

.1 Классификация методов и средств обеспечения безопасности

.2 Основные средства для создания механизмов защиты и информации

.3 Физическая защита данных в КС

.4 Программно-технические средства в сетях

.5 Практическое применение методов и средств сетевой безопасности

. Экономическая часть

.1 Организационно-экономическое обоснование

.2 Расчет себестоимости

.3 Трудоемкость производства

.4 Экономическая эффективность

Вывод

Заключение

Список используемых источников

Список сокращений

Глоссарий

Приложения

Введение

Проблема защиты информации является далеко не новой. Решать её люди пытались с древних времен.

На заре цивилизации ценные сведения сохранялись в материальной форме: вырезались на каменных табличках, позже записывались на бумагу. Для их защиты использовались такие же материальные объекты: стены, рвы.

Информация часто передавалась с посыльным и в сопровождении охраны. И эти меры себя оправдывали, поскольку единственным способом получения чужой информации было ее похищение. К сожалению, физическая защита имела крупный недостаток. При захвате сообщения враги узнавали все, что было написано в нем. Еще Юлий Цезарь принял решение защищать ценные сведения в процессе передачи. Он изобрел шифр Цезаря. Этот шифр позволял посылать сообщения, которые никто не мог прочитать в случае перехвата.

Данная концепция получила свое развитие во время Второй мировой войны. Германия использовала машину под названием Enigma для шифрования сообщений, посылаемых воинским частям.

Актуальность темы данной работы определяется в том, что вопросы защиты информации в сетях всегда были и есть очень важными, безопасность информации в сети - это одна из главных составляющих ее надлежащего функционирования. Методы и средства такой защиты информации должны постоянно совершенствоваться, учитывая новые возникающие угрозы безопасности сети. Поэтому вопросы методов и средств защиты информации в сетях оставались и остаются актуальными, пока существуют угрозы безопасности информации в сетях.

Развитие глобальной сети Интернет и сопутствующих технологий достигло такого высокого уровня, что сегодняшнюю деятельность любого предприятия в целом и каждого пользователя в отдельности, уже невозможно представить без электронной почты, Web-рекламы, общения в режиме "он-лайн".

В современном обществе информация может быть не только помощником, но и оружием. Распространение компьютерных систем и объединение их в коммуникационные сети усиливает возможности электронного проникновения в них. Во всех странах мира существует проблема компьютерной преступности, что вызывает необходимость привлечения все большего внимания и сил для организации борьбы с данным видом преступлений. Особенно большой размах преступления получили в автоматизированных банковских системах и в электронной коммерции. По зарубежным данным, потери в банках в результате компьютерных преступлений ежегодно составляют многие миллиарды долларов.

В связи с массовым внедрением компьютеров во все сферы деятельности человека объем информации, которая хранится в электронном виде, вырос в тысячи раз, а с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру не дает гарантии сохранности информационных ресурсов. Все больше появляется специализированных средств защиты информации, которые ориентированы на решение, как правило, только одной задачи обеспечения безопасности системы или в редких случаях, некоторого ограниченного набора задач. Так, организациям, чтобы оградить себя от "компьютерных" преступлений приходится реализовывать целый набор мер. Расширение применения современных информационных технологий делает возможным распространение различных злоупотреблений, связанных с использованием вычислительной техники.

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем на сегодняшний день.

Для уменьшения ущерба нужно грамотно выбирать меры и средства обеспечения защиты информации от кражи, умышленного разрушения, несанкционированного доступа, порчи, чтения и копирования. Необходимо знание основных законодательных положений в этой области, экономических, организационных и иных мер.

Технологии компьютерных систем и сетей развиваются очень быстро и, соответственно, также быстро появляются новые способы защиты информации.

Основной целью работы является изучение и анализ методов управления средствами сетевой безопасности, а именно основных вопросов и понятий защиты информации в сетях, видов угроз безопасности информации в сетях, не только программных, но и правовых методов и средств защиты. Необходимо рассмотреть и конкретные вопросы программной защиты информации в корпоративных сетях, существующие программные решения в этой области.

Исходя из поставленных в работе целей, которые требуется достичь, установим основные задачи, которые необходимо будет выполнить:

- рассмотреть основные понятия безопасности информации в сетях и виды существующих угроз;
- определить некоторые особенности безопасности компьютерных

сетей;

- проанализировать основные методы управления средствами сетевой безопасности;
- изучить существующие конкретные средства и методы программной защиты информации в сетях, особенностей защиты в различных сетях;
- проанализировать потенциальные угрозы в компьютерных сетях при реализации программных злоупотреблений.

1. Теоретические основы безопасности и защиты информации в компьютерных сетях

.1 Сущность проблемы и задачи защиты в компьютерных сетях

К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации.

Защитой информации называют деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Наиболее остро необходимость в защите данных проявляется при использовании компьютеров для обработки, а также хранения информации секретного и частного характера.

Проблема обеспечения необходимого уровня защиты информации оказалась весьма сложной, требующей для своего решения создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации. То есть становится актуальна проблема разработки эффективных систем защиты информации.

Основные проблемы защиты информации при работе в компьютерных сетях, можно разделить на три группы:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение работоспособности информационно-вычислительных систем.

Наиболее перспективными средствами защиты информации в

компьютерных системах являются программные средства. Они позволяют создать модель защищенной системы с построением правил разграничения доступа, централизованно управлять процессами защит, интегрировать различные механизмы в единую систему, создавать удобный для пользователей интерфейс администратора безопасности.

Не смотря на явные преимущества обработки информации в компьютерных сетях, возникает немало сложностей при организации их защиты:

- расширенная зона контроля - следовательно, администратору отдельной подсети приходится контролировать деятельность пользователей, которые находятся вне пределов его досягаемости;
- неизвестный периметр - сети легко расширяются, и это ведет к тому, что определить четкие границы сети часто бывает сложно, один и тот же узел может быть доступен для пользователей различных сетей;
- использование разнообразных программно-аппаратных средств - соединение нескольких систем в сеть увеличивает уязвимость всей системы в целом, так как каждая система настроена на выполнение своих требований безопасности, которые могут оказаться несовместимы с требованиями на других системах;
- сложность в управлении и контроле доступа к системе - многие атаки на сеть могут осуществляться из удаленных точек без получения физического доступа к определенному узлу. В таких случаях идентификация нарушителя, как правило, бывает очень сложной;
- множество точек атаки - один и тот же набор данных в сетях может передаваться через несколько промежуточных узлов, причем, каждый из этих узлов является возможным источником угрозы. Кроме этого, к большинству сетей можно получить доступ с помощью коммутируемых

линий связи и модема, что сильно увеличивает количество возможных точек атаки. Такой способ очень легко осуществить и столь же трудно проконтролировать, поэтому он считается одним из самых опасных. Уязвимыми местами сети также являются линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т.д.

Суть проблемы защиты сетей обусловлена их двойственным характером. С одной стороны, сеть - это единая система с едиными правилами обработки информации, а с другой, - совокупность отдельных систем, каждая из которых имеет свои собственные правила обработки информации.

.2 Угрозы, атаки и каналы утечки информации

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником.

Угроза чаще всего появляется вследствие наличия уязвимых мест в защите информационных систем (в качестве примера можно привести возможность доступа постороннего лица к критически важному оборудованию или какие-либо ошибки в программном обеспечении). Промежуток времени от момента, когда имеется возможность использовать слабое место, и до того момента, когда эта возможность ликвидируется, называют окном опасности, которое ассоциируется с данным уязвимым

местом. До тех пор пока существует окно опасности, будут возможны успешные атаки на информационную систему.

Одна из самых простых классификаций (когда все множество потенциальных угроз компьютерной информации можно представить по природе их возникновения) приведена на рисунке 1.

Рисунок 1. Общая классификация угроз безопасности.

Естественные угрозы - это угрозы, вызванные воздействиями на компьютерную систему и ее элементы каких-либо физических процессов или стихийных природных явлений, которые не зависят от человека. Среди них можно выделить:

- природные - это ураганы, наводнения, землетрясения, цунами, пожары, извержения вулканов, снежные лавины, селевые потоки, радиоактивные излучения, магнитные бури;
- технические - угрозы этой группы связаны с надежностью технических средств обработки информации.

Искусственные угрозы - это угрозы компьютерной системы, которые вызваны деятельностью человека. Среди них можно выделить:

- непреднамеренные угрозы, которые вызваны ошибками людей при проектировании компьютерной системы, а также в процессе ее эксплуатации;
- преднамеренные угрозы, связанные с корыстными устремлениями людей. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть

обусловлены разными мотивами: недовольство служащего своей карьерой; взятка; любопытство; конкурентная борьба; стремление самоутвердиться любой ценой.

Можно составить предполагаемую модель возможного нарушителя:

- квалификация нарушителя соответствует уровню разработчика данной системы;
- нарушителем может быть как законный пользователь системы, так и постороннее лицо;
- нарушителю известна принципиальная работы системы;
- нарушитель выбирает наиболее слабое звено в защите.

Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена.

Общая схема классификации угроз информационной безопасности компьютерных сетей приведена в приложении А.

Угрозы в компьютерных сетях можно классифицировать следующим образом.

По цели реализации угрозы могут быть нарушающими целостность информации (что может привести к утрате или обесцениванию информации); нарушающими конфиденциальность информации (что может нанести значительный ущерб ее владельцам); нарушающими доступность компьютерной сети.

По принципу воздействия на сеть угрозы подразделяются на использующие скрытые каналы (обмен информацией таким способом,

нарушает системную политику безопасности); использующие доступ субъекта компьютерной сети к объекту (доступ - это взаимодействие между субъектом и объектом, приводящее к возникновению информационного потока от второго к первому).

По характеру воздействия на сеть - активное воздействие, связано с выполнением нарушителем каких-либо действий, например, доступ к определенным наборам данных, вскрытие пароля, доступ к программам и т.д. Такое воздействие ведет к изменению состояния сети. Пассивное воздействие, осуществляется с помощью наблюдения за какими-либо побочными эффектами и их анализом. Пассивное воздействие не ведет к изменению состояния системы, т.к. оно всегда связано только с нарушением конфиденциальности информации в компьютерных сетях (никаких действий с субъектами и объектами не производится).

По способу активного воздействия на объект атаки возможно непосредственное воздействие (с помощью средств контроля доступа такое действие достаточно легко предотвратить); воздействие на систему разрешений (несанкционированные действия осуществляются относительно прав на объект атаки, а сам доступ к объекту выполняется потом законным образом); опосредованное воздействие (в качестве примера можно рассмотреть случай, когда злоумышленник выдает себя за авторизованного пользователя, каким-либо образом присвоив себе его полномочия.).

По используемым средствам атаки - с использованием стандартных программ (в этом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ хорошо изучены); с использованием специально разработанных программ, что может быть более опасным для сети.

По состоянию объекта атаки - когда в момент атаки объект находится в

состоянии хранения информации (в таком случае воздействие на объект, как правило, осуществляется с использованием несанкционированного доступа); в момент осуществления передача информации по линии связи между узлами сети или внутри узла (в таком случае воздействие на объект предполагает либо доступ к фрагментам передаваемой информации, либо прослушивание с использованием скрытых каналов); объект находится в состоянии обработки информации (здесь объект атаки - это процесс пользователя).

Кроме перечисленных угроз информационной безопасности следует добавить следующие угрозы:

- несанкционированный обмен информацией между пользователями;
- отказ от информации;
- отказ в обслуживании.

Компьютерные сети характерны тем, что против них можно осуществить удаленные атаки. Нападению может подвергнуться и конкретный компьютер, и информация, передающаяся по сетевым каналам связи, хотя нарушитель в это время может находиться за много километров от атакуемого объекта.

Атака на сеть может производиться с верхнего уровня (когда нарушитель использует свойства сети для проникновения на другой узел и выполнения определенных несанкционированных действий) и нижнего уровня (нарушитель использует свойства сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом).

Выделяют четыре основных категории атак:

- атаки доступа - злоумышленник пытается получить информацию, на просмотр которой у него нет разрешений. Везде, где существует

информация и средства для ее передачи возможно выполнение такой атаки. Атака доступа нарушает конфиденциальность информации;

- атаки модификации - направлены на нарушение целостности информации. Такие атаки возможна везде, где существует или передается информация;
- атаки на отказ от обязательств - такая атака направлена против возможности идентифицировать информацию, говоря другими словами, это попытка дать неверную информацию о реальном событии или транзакции;
- атаки на отказ в обслуживании (Denial-of-service, DoS) - это атаки, приводящие к невозможности получения информации легальным пользователям. В результате DoS-атаки злоумышленник обычно не получает доступа к компьютерной системе и не может оперировать с информацией, он просто делает систему или находящуюся в ней информацию недоступной.

Имеется огромное множество способов выполнения атак: при помощи специально разработанных средств, через уязвимые места компьютерных систем. Одним из наиболее опасных способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Наиболее распространенными видами вредоносных программ являются "троянские кони", черви и вирусы.

"Троянский конь" - это вредоносная программа, которая используется злоумышленником для сбора информации, её разрушения или модификации, а также нарушает работоспособность компьютера или использует его ресурсы в неблаговидных целях. Чаще всего троянский конь маскируется под новую версию бесплатной утилиты, какую-то популярную прикладную программу или игру. Таким способом пытается заинтересовать пользователя и побудить его переписать и установить на свой компьютер вредителя самостоятельно.

Компьютерный вирус - вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Сетевой червь - разновидностьвредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

Свое название компьютерные вирусы получили из-за определенного сходства с биологическими вирусами, такими как: способность к саморазмножению; высокая скорость распространения; избирательность поражаемых систем; наличие в большинстве случаев инкубационного периода; способность "заражать" еще незараженные системы; трудность борьбы с вирусами и т.д.

В последнее время к этим особенностям добавилась еще и постоянно увеличивающаяся быстрота появления модификаций и новых поколений вирусов, что можно объяснить идеями злоумышленников определенного склада ума.

Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-либо вредные действия.

Процесс заражения вирусом программных файлов можно представить следующим образом. В зараженной программе код последней изменяется

таким образом, чтобы вирус получил управление первым, до начала работы программы-вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы. Если вирус записывается в конец программы, то он корректирует код программы с тем, чтобы получить управление первым. После этого управление передается программе-вирусоносителю, и та нормально выполняет свои функции. Более изощренные вирусы могут для получения управления изменять системные области накопителя (например, сектор каталога), оставляя длину и содержимое заражаемого файла без изменений.

Евгений Касперский - один из самых авторитетных "вирусологов" страны предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Более подробная классификация внутри этих групп представлена в приложении Б.

В настоящее время вредоносное программное обеспечение очень разнообразно и представляет собой серьезную угрозу. К тому же, все чаще речь идет не только об удаленных с жесткого диска файлах или испорченной операционной системе. Современные вирусы и троянские кони наносят огромный материальный ущерб и позволяют их создателям и распространителям зарабатывать деньги. Это приводит к тому, что вредоносное программное обеспечение развивается очень активно.

В основном атаки, нацеленные на захват информации, хранимой в

электронном виде, имеют одну интересную особенность: информация не похищается, а копируется. Она остается у исходного владельца, но при этом ее получает и злоумышленник. Таким образом, владелец информации несет убытки, а обнаружить момент, когда это произошло, очень трудно.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД). НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Несанкционированный доступ к информации, находящейся в сети может быть косвенным (без физического доступа к элементам сети) или прямым (с физическим доступом к элементам сети).

Канал утечки информации - это совокупность источников информации, материального носителя или среды распространения несущего эту информацию сигнала и средства выделения информации из сигнала или носителя.

Основные каналы утечки информации:

1. Электромагнитный канал. Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в технических средствах обработки информации. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки).

Электромагнитный канал в свою очередь делится на: радиоканал (высокочастотные излучения); низкочастотный канал; сетевой канал (наводки на провода заземления); канал заземления (наводки на провода заземления); линейный канал (наводки на линии связи между компьютерами).

. Акустический канал. Он связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе

устройств отображения информации.

. Канал несанкционированного копирования.

. Канал несанкционированного доступа.

.3 Методы обеспечения безопасности сетей

Рассмотрим конкретные методы и средства защиты, которые используются в компьютерных сетях.

Парольная защита основывается на том, что для того, чтобы использовать какой-либо ресурс, необходимо задать пароль (некоторая комбинация символов). С помощью паролей защищаются файлы, архивы, программы и отдельные компьютеры. У парольной защиты есть недостатки - это слабая защищенность коротких паролей, которые с помощью специальных программ можно быстро раскрыть простым перебором. При выборе пароля нужно соблюдать ряд требований: пароль не должен состоять менее, чем из восьми символов; не использовать один и тот же пароль для доступа к разным ресурсам; не использовать старый пароль повторно; менять пароль как можно чаще. В сетях пароли могут использоваться самостоятельно, а также в качестве основы для различных методов аутентификации.

Идентификацию и аутентификацию пользователей можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов.

Идентификация представляет собой процедуру распознавания пользователя (процесса) по его имени.

Аутентификация - это процедура проверки подлинности пользователя, аппаратуры или программы для получения доступа к определенной

информации или ресурсу.

В качестве синонима слова "аутентификация" иногда используют сочетание "проверка подлинности". Субъект может подтвердить свою подлинность, если предъявит, по крайней мере, одну из следующих сущностей:

- нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.,
- нечто, чем он владеет: личную карточку или иное устройство аналогичного назначения,
- нечто, что является частью его самого: голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики,
- нечто, ассоциированное с ним, например координаты.

Криптографические методы защиты основываются на шифровании информации и программ. Готовое к передаче сообщение - будь то данные, речь либо графическое изображение того или иного документа, обычно называется открытым, или незащищенным текстом. Такое сообщение в процессе передачи по незащищенным каналам связи может быть легко перехвачено. Для предотвращения несанкционированного доступа к сообщению оно зашифровывается, преобразуясь в закрытый текст. Санкционированный пользователь, получив сообщение, дешифрует его обратным преобразованием криптограммы. В результате чего получается исходный открытый текст.

Шифрование может быть симметричным и асимметричным. Симметричное шифрование использует один и тот же секретный ключ для шифровки и дешифровки. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это ставит новую проблему

рассылки ключей. С другой стороны, получатель, имеющий шифрованное и расшифрованное сообщение, не может доказать, что он получил его от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать и сам.

При ассиметричном шифровании для шифрования используется один общедоступный ключ, а для дешифрования - другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Асимметричные методы шифрования позволяют реализовать так называемую электронную подпись. Идея состоит в том, что отправитель посылает два экземпляра сообщения - открытое и дешифрованное его секретным ключом. Получатель может зашифровать с помощью открытого ключа отправителя дешифрованный экземпляр и сравнить с открытым ключом. Если они совпадут, личность и подпись отправителя можно считать установленными.

Существенным недостатком асимметричных методов является их низкое быстродействие, поэтому их приходится сочетать с симметричными. Так, для решения задачи рассылки ключей сообщение сначала симметрично шифруют случайным ключом, затем этот ключ шифруют открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

При использовании асимметричных методов необходимо иметь гарантию подлинности пары (имя, открытый ключ) адресата. Для решения этой задачи вводится понятие сертификационного центра, который заверяет справочник имен/ключей своей подписью.

Шифрование программ гарантирует невозможность внесения в них изменений. Криптографическая защита данных осуществляется и при

хранении данных и при передаче их по сети. В настоящее время возможна как программная, так и аппаратная реализация средств криптографии.

Привязка программ и данных к конкретному компьютеру (сети или ключу). Идея этого метода заключается в том, чтобы включить в данные или в программу параметры или характеристики конкретного компьютера, что сделает невозможным чтение данных или выполнение программ на другом компьютере. Различные модификации этого метода применительно к сети могут требовать или выполнение всех операций на конкретном компьютере, или активного соединения сети с конкретным компьютером. Метод "привязки" может значительно повысить защищенность сети.

Разграничение прав доступа пользователей к ресурсам сети. Этот метод основан на использовании наборов таблиц, которые определяют права пользователей. Они построены по правилам "разрешено все, кроме" или "разрешено только". Таблицы по паролю или идентификатору пользователя определяют его права доступа к дискам, файлам, операциям чтения, записи, копирования, удаления и другим сетевым ресурсам. Такое разграничение доступа определяется, как правило, возможностями используемой ОС.

Управление доступом может быть достигнуто при использовании дискреционного или мандатного управления доступом.

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретного субъекта. Правом редактирования дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности. Эта модель отличается простотой реализации, но возможна утечка конфиденциальной информации даже в результате санкционированных действий пользователей.

Мандатная модель разграничения доступа предполагает назначение

объекту метки (грифа) секретности, а субъекту - уровня допуска. Доступ субъектов к объектам в мандатной модели определяется на основании правил "не читать выше" и "не записывать ниже". Использование мандатной модели, в отличие от дискреционного управления доступом, предотвращает утечку конфиденциальной информации, но снижает производительность компьютерной системы.

Протоколирование и аудит состояния системы безопасности составляют основу обеспечения безопасности корпоративной сети.

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе предприятия.

Аудит - это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие главные цели:

- обеспечение подотчетности пользователей и администраторов - обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений. Тем самым обеспечивается целостность информации;
- обеспечение возможности реконструкции последовательности событий - позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем - позволяют помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или

перенастроить систему, снова измерить производительность и т.д.

Аудит информационной безопасности является сегодня одним из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищённости предприятия от угроз информационной безопасности. Кроме того, результаты аудита используются для формирования стратегии развития системы защиты информации в организации. Необходимо помнить, что аудит безопасности не является однократной процедурой, а должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную пользу и способствовать повышению уровня информационной безопасности компании.

Межсетевое экранирование

При подключении корпоративной сети к открытым сетям, например к сети Internet, появляются угрозы несанкционированного вторжения в закрытую (внутреннюю) сеть из открытой (внешней), а также угрозы несанкционированного доступа из закрытой сети к ресурсам открытой. Подобный вид угроз характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации разного уровня секретности.

Нарушитель через открытую внешнюю сеть может вторгнуться в сеть организации и получить доступ к техническим ресурсам и конфиденциальной информации, получить пароли, адреса серверов, а иногда и их содержимое, войти в информационную систему организации под именем зарегистрированного пользователя и т.д.

Угрозы несанкционированного доступа из внутренней сети во внешнюю сеть являются актуальными в случае ограничения разрешенного доступа во внешнюю сеть правилами, установленными в организации.

Ряд задач по отражению угроз для внутренних сетей способны решить межсетевые экраны.

Межсетевой экран (МЭ) или брандмауэр (Firewall) - это средство защиты, которое можно использовать для управления доступом между надежной сетью и менее надежной. Основная функция МЭ - централизация управления доступом. Если удаленные пользователи могут получить доступ к внутренним сетям в обход МЭ, его эффективность близка к нулю. МЭ обычно используются для защиты сегментов локальной сети организации.

Межсетевые экраны обеспечивают несколько типов защиты:

- блокирование нежелательного трафика;
- перенаправление входного трафика только к надежным внутренним системам;
- сокрытие уязвимых систем, которые нельзя обезопасить от атак из глобальной сети другим способом;
- протоколирование трафика в и из внутренней сети;
- сокрытие информации (имен систем, топологии сети, типов сетевых устройств и внутренних идентификаторов пользователей, от внешней сети;
- обеспечение более надежной аутентификации, чем та, которую представляют стандартные приложения.

Как и для любого средства защиты, нужны определенные компромиссы между удобством работы и безопасностью. Прозрачность - это видимость МЭ как внутренним пользователям, так и внешним, осуществляющим взаимодействие через МЭ, который прозрачен для пользователей, если он не мешает им получить доступ к сети.

Обычно МЭ конфигурируются так, чтобы быть прозрачными для внутренних пользователей сети (посылающим пакеты наружу), и, с другой

стороны, МЭ конфигурируется так, чтобы быть непрозрачным для внешних пользователей, пытающихся получить доступ к внутренней сети извне. Это обычно обеспечивает высокий уровень безопасности и не мешает внутренним пользователям.

Важным понятием экранирования является зона риска, определяемая как множество систем, которые становятся доступными злоумышленнику после преодоления экрана или какого-либо из его компонентов.

Для повышения надежности защиты, экран реализуют как совокупность элементов, так что "взлом" одного из них еще не открывает доступ ко всей внутренней сети.

Экранирование и с точки зрения сочетания с другими сервисами безопасности, и с точки зрения внутренней организации использует идею многоуровневой защиты, за счет чего внутренняя сеть оказывается в пределах зоны риска только в случае преодоления злоумышленником нескольких, по-разному организованных защитных рубежей.

Экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями.

1.4 Правовые аспекты защиты информации

Обзор российского законодательства в области информационной безопасности

Требования российского законодательства, определяющие обязательность защиты информации ограниченного доступа, изложены в Федеральных иконах и уточнены в документах Федеральной службы по техническому и экспортному контролю Российской Федерации ФСБ

(ФАПСИ) и других государственных учреждений, имеющих отношение к обеспечению безопасности информации. Реализация и контроль этих требований осуществляется при помощи соответствующих государственных систем сертификации средств защиты и аттестации объектов автоматизации.

Правовую основу информационной безопасности обеспечивают: Конституция Российской Федерации, Гражданский и Уголовный Кодекс, Федеральные законы "О безопасности" (№15-ФЗ от 07.03.2005), "О Государственной тайне" (№122-ФЗ от 22.08.2004), "Об информации, информатизации и защите информации" (№ 149-ФЗ от 27.07.2006), "Об участии в международном информационном обмене" (№85-ФЗ от 04.07.1996), "О коммерческой тайне" (№98-ФЗ от 29.07.2004), "О персональных данных" (№152-ФЗ от 27.07.2006), "О техническом регулировании" (№45-ФЗ от 09.05.2005), Доктрина информационной безопасности, Указы Президента и другие нормативные правовые акты Российской Федерации.

Соблюдение правовых норм, установленных законодательными актами Российской Федерации, должно являться одним из основополагающих принципов при создании любой комплексной системы защиты от информационных атак.

Общие правовые основы обеспечения безопасности личности, общества и государства определены в Федеральном законе "О безопасности". Этим же законом определено понятие системы безопасности и ее функций, установлен порядок организации и финансирования органов обеспечения безопасности и правила контроля и надзора за законностью их деятельности.

Основные положения государственной политики в сфере обеспечения безопасности изложены в Доктрине информационной безопасности Российской Федерации. В Доктрине определены следующие основные задачи, которые необходимо учитывать при реализации комплекса мер по

информационной безопасности:

- 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 условий 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, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России;
- обеспечение защиты сведений, составляющих государственную тайну.

В соответствии с Конституцией Российской Федерации (ст. 23, 24) мероприятия по защите данных от возможных информационных атак не должны нарушать тайну переписки, осуществлять сбор сведений о частной жизни сотрудников, а также ознакомление с их перепиской.

В Гражданском кодексе Российской Федерации (ст. 139) определены характерные признаки информации, которая может составлять служебную или коммерческую тайну. Кроме этого в гражданском кодексе установлена ответственность, которую несут лица, за незаконные методы получения такой информации.

Уголовным Кодексом Российской Федерации предусматривается ответственность в случае преднамеренного использования вредоносного программного обеспечения с целью:

- сбора или распространения сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия (ст. 137);
- незаконного получения или разглашения сведений, составляющих коммерческую или банковскую тайну (ст. 183);
- неправомерного доступа к охраняемой законом компьютерной информации (ст. 272);
- нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (ст. 274);
- нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, с использованием специальных технических средств, предназначенных для негласного получения информации (ст. 138).

Уголовная ответственность распространяется также на лиц, совершивших действия по созданию, использованию и распространению вредоносных программ для ЭВМ (ст. 273). При этом необходимо отметить, что в качестве вредоносного ПО могут выступать не только вирусы, программы типа "Троянский конь", но и программы, предназначенные для проведения информационных атак.

Регулирование отношений, связанных с созданием, правовой охраной, а также использованием программ для ЭВМ и баз данных, осуществляется при помощи законов "О правовой охране программ для электронных вычислительных машин и баз данных" и "Об авторском праве и смежных правах".

Федеральный закон "Об участии в международном информационном обмене" также определяет понятие информационной безопасности и направлен на создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства. Требования данного нормативного документа необходимо учитывать при взаимодействии с зарубежными информационными ресурсами, например, через сеть Интернет. Отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления и предоставления потребителю документированной информации, регулируются Федеральным законом "Об информации, информатизации и защите информации".Данный закон определяет понятие конфиденциальной информации, цели и задачи по ее защите, а также права и обязанности субъектов в области защиты информации. В 2006 г. эти два закона были заменены Федеральным законом "Об информации, информационных технологиях и о защите информации",в соответствии с которым защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Более подробно информация конфиденциального характера определена в Указе Президента Российской Федерации №188 от 06.03.1997 г. "Об утверждении перечня сведений конфиденциального характера". В

соответствии с данным Указом к подобным сведениям отнесены:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Более подробные сведения об информации, составляющей коммерческую тайну, изложены в Федеральном законе "О коммерческой тайне".Данный Закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации и других участников регулируемых отношений на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

Вопросы защиты персональных данных подробно описаны в Федеральном законе "О персональных данных". В соответствии с этим документом при обработке персональных данных необходимо принимать организационные и технические меры, в том числе криптографические средства для защиты информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,

распространения персональных данных, а также от иных неправомерных действий.

Вопросы отнесения информации к государственной тайне, а также порядок работы и защиты таких данных определены в Федеральном законе "О государственной тайне". Статьи закона являются обязательными для исполнения для всех без исключения юридических и физических лиц, для государственных и территориальных органов власти. Закон определяет понятия государственной тайны, грифа секретности, средства защиты информации и др. Этот же закон устанавливает права и обязанности органов государственной власти по защите государственной тайны, а также определяет базовый перечень сведений, которые могут быть отнесены к государственной тайне. Более подробный перечень утвержден Указом Президента "О перечне сведений, отнесенных к государственной тайне" №61 от 28.03.1998 г. Данные нормативные документы должны учитываться при формировании системы защиты информации, составляющей государственную тайну.

Нормативно-методическую базу, определяющую требования и рекомендации к программно-техническим методам защиты информации в автоматизированных системах, составляют руководящие документы Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК) и государственные стандарты. Так, например, оценка защищенности автоматизированных систем, обрабатывающих информацию ограниченного доступа, осуществляется на основании руководящего документа (РД) ФСТЭК "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации". При разработке и модернизации средств вычислительной техники необходимо

принимать во внимание требования РД ФСТЭК "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" и ГОСТ Р 50739-95"Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования". Данные нормативные документы необходимо учитывать в процессе реализации комплексной системы защиты от информационных атак для того, чтобы не нарушить установленные в них требования к автоматизированным системам и средствам вычислительной техники соответствующих классов.

Еще одним нормативным документом ФСТЭК, который может применяться по отношению к средствам защиты от информационных атак, является РД "Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ)". Данный РД устанавливает классификацию ПО средств защиты информации по уровню контроля отсутствия в нем НДВ. Необходимо отметить, что под НДВ понимают функциональные возможности ПО, не описанные в документации, при использовании которых возможно нарушение конфиденциальности, целостности или доступности обрабатываемой информации.

При использовании персональных и корпоративных межсетевых экранов для защиты от информационных атак необходимо учитывать требования РД ФСТЭК "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации" ,а также "требования ФСБ к устройствам типа межсетевые экраны".Данные нормативные документы классифицируют межсетевые экраны на пять

различных классов в зависимости от категории информации, для защиты которой они предназначены. При этом каждый класс экранов характеризуется своим набором функциональных требований по защите информации.

Порядок организации работ с государственной конфиденциальной информацией определяется в нормативно-методическом документе ФСТЭК "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)". Документ расширяет и дополняет существующие РД посредством уточнения требований и рекомендаций по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. В этом документе приводятся рекомендации по практическому применению различных средств защиты, в том числе и систем обнаружения атак.

2. Методы и средства защиты информации в сетях

.1 Классификация методов и средств обеспечения безопасности

Способы (методы) защиты информации:

- Препятствие - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
- Управление - оказание управляющих воздействий на элементы защищаемой системы.
- Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника.
- Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.
- Принуждение - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)
- Побуждение - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

Средства защиты информации:

- Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и т. п.

устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

- Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемновстраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.
- Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.
- Организационные средства - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.
- Законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.
- Психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

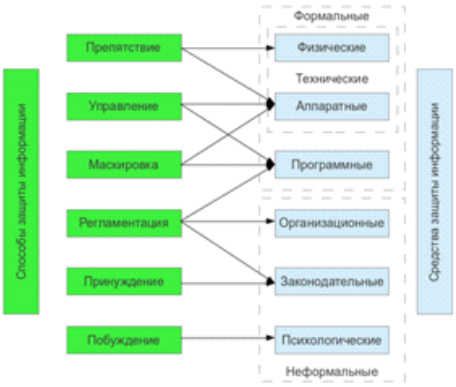


Рисунок 2. Классификация методов и средств защиты информации

2.2 Основные средства для создания механизмов защиты и информации

Рассмотрим, какие существуют средства или инструменты, которыми реализованы описанные принципы или механизмы. Персонал занимается аудитом, который обеспечивает учет. Значит, персонал - это средство, аудит - механизм, а учет - цель. Или пароли, обеспечивающие аутентификацию, сохраняются в шифрованном виде, аутентификация предшествует, например, разрешению на модификацию. Значит, криптография - средство защиты паролей, пароли используются для механизма аутентификации, аутентификация предшествует обеспечению целостности.

Основные средства (инструменты) информационной безопасности:

- персонал - люди, которые будут обеспечивать претворение в жизнь информационной безопасности во всех аспектах, то есть разрабатывать, внедрять, поддерживать, контролировать и исполнять;
- нормативное обеспечение - документы, которые создают правовое пространство для функционирования информационной безопасности;
- модели безопасности - схемы обеспечения информационной безопасности, заложенные в данную конкретную информационную систему или среду;
- криптография - методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей - специальных информационных объектов, реализующих эти санкции;
- антивирусное обеспечение - средство для обнаружения и

уничтожения зловредного кода (вирусов, троянских программ и т.п.);

- межсетевые экраны - устройства контроля доступа из одной информационной сети в другую;
- сканеры безопасности - устройства проверки качества функционирования модели безопасности для конкретной информационной системы;
- системы обнаружения атак - устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности;
- резервное копирование - сохранение избыточных копий информационных ресурсов на случай их возможной утраты или повреждения;
- дублирование (резервирование) - создание альтернативных устройств, необходимых для функционирования информационной среды, предназначенных для случаев выхода из строя основных устройств;
- аварийный план - набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности;
- обучение пользователей - подготовка активных участников информационной среды для работы в условиях соответствия требованиям информационной безопасности.

Основные направления информационной безопасности.

Физическая безопасность - обеспечение сохранности самого оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию.

Компьютерная безопасность (сетевая безопасность, телекоммуникационная безопасность, безопасность данных) - обеспечение

защиты информации в ее виртуальном виде. В конкретном программном комплексе модель безопасности может быть реализована таким образом, что это потребует отдельного специалиста (или даже службы) по ее поддержанию. В этом случае, возможно разделить понятия безопасность данных (конкретного приложения) и безопасность сети (всей остальной информационной среды).

.3 Физическая защита данных в КС

Кабельная система

Кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим способом является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охранных систем. К структурированным кабельным системам относятся, например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании Digital, кабельная система корпорации IBM.

Понятие "структурированность" означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и месторасположения компонентов кабельной системы. Например, кабельная система SYSTIMAX SCS состоит из:

- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.
- Внешней подсистемы (campus subsystem)
- Аппаратных (equipment room)
- Административной подсистемы (administrative subsystem)
- Магистрали (backbone cabling)
- Горизонтальной подсистемы (horizontalsubsystem)

Внешняя подсистема состоит из медного и оптоволоконного кабеля,

устройств электрической защиты и заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании (или комплексе зданий). Кроме того, в эту подсистему входят устройства сопряжения внешних кабельных линий с внутренними.

Аппаратные служат для размещения различного коммуникационного оборудования, предназначенного для обеспечения работы административной подсистемы.

Административная подсистема предназначена для быстрого и легкого управления кабельной системой SYSTIMAX SCS при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкранированная витая пара и оптоволокно), устройства коммутации и сопряжения магистрали и горизонтальной подсистемы, соединительные шнуры, маркировочные средства и т.д.

Магистраль состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она связывает между собой этажи здания или большие площади одного и того же этажа.

Горизонтальная система на базе витого медного кабеля расширяет основную магистраль от входных точек административной системы этажа к розеткам на рабочем месте.

Оборудование рабочих мест включает в себя соединительные шнуры, адаптеры, устройства сопряжения и обеспечивает механическое и электрическое соединение между оборудованием рабочего места и горизонтальной кабельной подсистемой.

Наилучшим способом защиты кабеля от физических (а иногда и температурных и химических воздействий, например, в производственных цехах) является прокладка кабелей с использованием в различной степени защищенных коробов. При прокладке сетевого кабеля вблизи источников

электромагнитного излучения необходимо выполнять следующие требования:

- неэкранированная витая пара должна отстоять минимум на 15-30 см от электрического кабеля, розеток, трансформаторов и т.д.
- требования к коаксиальному кабелю менее жесткие - расстояние до электрической линии или электроприборов должно быть не менее 10-15 см.

Другая важная проблема правильной инсталляции и безотказной работы кабельной системы - соответствие всех ее компонентов требованиям международных стандартов.

Наибольшее распространение в настоящее время получили следующие стандарты кабельных систем:

Спецификации корпорации IBM, которые предусматривают девять различных типов кабелей. Наиболее распространенным среди них является кабель IBM type 1 - экранированная витая пара (STP) для сетей TokenRing.

Система категорий UnderwritersLabs (UL) представлена этой лабораторией совместно с корпорацией Anixter. Система включает пять уровней кабелей. В настоящее время система UL приведена в соответствие с системой категорий EIA/TIA.

Стандарт EIA/TIA 568 был разработан совместными усилиями UL, American National Standards Institute (ANSI) и Electronic Industry Association/Telecommunications Industry Association, подгруппой TR41.8. 1 для кабельных систем на витой паре (UTP).

Необходимо также отметить, что требования стандарта EIA/TIA 568 относятся только к сетевому кабелю. Но реальные системы, помимо кабеля, включают также соединительные разъемы, розетки, распределительные панели и другие элементы. Использование только кабеля категории 5 не

гарантирует создание кабельной системы этой категории. В связи с этим все вышеперечисленное оборудование должно быть также сертифицировано на соответствие данной категории кабельной системы.

Системы электроснабжения

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания. Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и т.д. - оснащены собственными дублированными системами электропитания.

Системы архивирования и дублирования информации

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Такой сервер автоматически производит архивирование информации с жестких дисков серверов и рабочих станций в указанное администратором локальной вычислительной сети время, выдавая отчет о проведенном

резервном копировании. При этом обеспечивается управление всем процессом архивации с консоли администратора, например, можно указать конкретные тома, каталоги или отдельные файлы, которые необходимо архивировать. Возможна также организация автоматического архивирования по наступлении того или иного события ("eventdrivenbackup"), например, при получении информации о том, что на жестком диске сервера или рабочей станции осталось мало свободного места, или при выходе из строя одного из "зеркальных" дисков на файловом сервере. Среди наиболее распространенных моделей архивационных серверов можно выделить StorageExpressSystem корпорации Intel, ARCserveforWindows, производства фирмы Cheyenne и ряд других.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия. Для обеспечения восстановления данных при сбоях магнитных дисков в последнее время чаще всего применяются системы дисковых массивов - группы дисков, работающих как единое устройство, соответствующих стандарту RAID (RedundantArraysofInexpensiveDisks). Эти массивы обеспечивают наиболее высокую скорость записи/считывания данных, возможность полного восстановления данных и замены вышедших из строя дисков в "горячем" режиме (без отключения остальных дисков массива).

Организация дисковых массивов предусматривает различные технические решения, реализованные на нескольких уровнях.

Уровень 0 предусматривает простое разделение потока данных между двумя или несколькими дисками. Преимущество подобного решения заключается в увеличении скорости ввода/вывода пропорционально

количеству задействованных в массиве дисков. В то же время такое решение не позволяет восстановить информацию при выходе из строя одного из дисков массива.уровня 1 заключается в организации так называемых "зеркальных" дисков. Во время записи данных информация основного диска системы дублируется на зеркальном диске, а при выходе из строя основного диска в работу тут же включается "зеркальный".

Уровни 2 и 3 предусматривают создание так называемых параллельных дисковых массивов, при записи на которые данные распределяются по дискам на битовом уровне. Специальный диск выделяется для сохранения избыточной информации, которая используется для восстановления данных при выходе из строя какого-либо из дисков массивов.

Уровни 4 и 5 представляют собой модификацию нулевого уровня, при котором поток данных распределяется по дискам массива. Отличие состоит в том, что на уровне 4 выделяется специальный диск для хранения избыточной информации, а на уровне 5 избыточная информация распределяется по всем дискам массива. Организация дисковых массивов в соответствии со стандартом 5 уровня обеспечивает высокую скорость считывания/записи информации и позволяет восстанавливать данные при сбое какого-либо диска без отключения всего дискового массива.

Среди всех вышеперечисленных уровней дисковых массивов уровни 3 и 5 являются наиболее предпочтительными и предполагают меньшие по сравнению с организацией "зеркальных" дисков материальные затраты при том же уровне надежности.

Повышение надежности и защита данных в сети, основанная на использовании избыточной информации, реализуются не только на уровне отдельных элементов сети, например дисковых массивов, но и на уровне сетевых ОС. Так, на протяжении последних десяти лет компания Novell

реализует отказоустойчивые версии операционной системы Netware - SFT (SystemFaultTolerance), предусматривающие три основных уровня:

- SFT Level I. Первый уровень предусматривает, в частности, создание дополнительных копий FAT и DirectoryEntriesTables, немедленную верификацию каждого вновь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска. При обнаружении сбоя данные перенаправляются в зарезервированную область диска, а сбойный блок помечается как "плохой" и в дальнейшем не используется.
- SFT Level II содержала дополнительно возможности создания "зеркальных" дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.
- Версия SFT Level III позволяет использовать в локальной сети дублированные серверы, один из которых является "главным", а второй, содержащий копию всей информации, вступает в работу в случае выхода "главного" сервера из строя.

2.4 Программно-технические средства в сетях

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными средствами принято понимать технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Например, система опознания и разграничения доступа к информации (посредством паролей, записи кодов и другой информации на различные карточки). Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, источники бесперебойного питания, электромеханическое оборудование охранной сигнализации. Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Все средства защиты информации от несанкционированного доступа можно подразделять на следующие группы:

- Технические (аппаратные) средства и системы независящие от объекта защиты, т.е. помещения, места расположения, рабочей станции и т.д.
- Программно-аппаратные средства и системы, выполненные как отдельное устройство функционирующие совместно с объектом защиты в определенной последовательности в соответствии с выполнением программного алгоритма
- Программные средства или системы (программы работы с BIOS, программные файерволы, антивирусные средства и т.д.) установленные на

рабочей станции и функционирующие в соответствии с выполнением собственных алгоритмов

Системы защиты информации при администрировании можно разделить следующим образом:

- Разграничение доступа к объекту защиты выполняется с применением идентификации (ввод имени пользователя, использования ключа доступа - дискеты, eToken-ключи, другие внешние аппаратных устройств);
- Аутентификация пользователя при доступе к защищаемой информации;
- Аудит доступа, ведение списка пользователей, блокирование доступа;
- Контроль целостности как папок и файлов, так и секторов и дисков;
- Аудит контроля целостности;
- Запрет и аудит загрузки с внешних или съемных носителей;
- Средство безопасной аутентификации eToken <http://dehack.ru/szi_nsd/prog_tech-prog_szi/etoken/>;
- Система защиты электронный замок "Соболь" <http://dehack.ru/szi_nsd/prog_tech-prog_szi/sobol/>;
- Система защиты информации "Страж NT <http://dehack.ru/szi_nsd/prog_tech-prog_szi/strazh_nt/>";
- Система защиты информации "SecretNet" <http://dehack.ru/szi_nsd/prog_tech-prog_szi/secretnet/>;
- Система защиты информации "Электронный замок "eLock" <http://dehack.ru/szi_nsd/prog_tech-prog_szi/elock/>;
- Система защиты информации "DallasLock" <http://dehack.ru/szi_nsd/prog_tech-prog_szi/dallas_lock/>;

Средство безопасной аутентификации eToken. Для государственных и коммерческих организаций сохранение конфиденциальной информации является одной из приоритетных задач. Организация эффективного и

защищенного доступа к информационным ресурсам является сложной задачей. Одним из решений является возможность получения доступа с помощью специализированных токенов (ключей). Однако, оптимальный выбор представляет собой проблему.

Для определения наиболее эффективного средства аутентификации рационально использовать метод анализа иерархий.

Метод анализа иерархий (МАИ) является методологической основой для решения задач выбора альтернатив посредством их многокритериального рейтингования. Зарубежные ученые использую МАИ в своих исследованиях.

Изучив рынок средств аутентификации, для анализа и последующего внедрения одного из данных средств были выбраны следующие: eToken PRO, iButton (DS1961S), ruToken, eToken PASS и eToken PRO Anywhere.

Приведем некоторые характеристики устройств, взятые с официальных сайтов.

- eToken PRO. Ключи eToken PRO являются персональным средством аутентификации и хранения данных. Рассматриваемые устройства аппаратно поддерживают работу с цифровыми сертификатами и электронно-цифровой подписью. Возможности eToken PRO: двухфакторная аутентификация пользователей; поддержка Java-апплетов; возможность централизованного управления. Цена от 947 р.
- iButton (DS1961S). iButton - это микросхема, вставленная в защищенный металлический корпус. Форма устройства в виде монеты позволяет простое использование оператором. Представленной электронный ключ используется для аутентификации пользователя, доступа в охраняемую зону. Возможности iButton(DS1961S): цифровая идентификация; обеспечение компактности хранения информации; передача информации при контакте. Цена - 130 р.

- ruToken. Данный идентификатор является компактным устройством в виде USB-брелка, который используется для авторизации пользователя, защиты электронной переписки, удаленного доступа к ресурсам, безопасного и надежного хранения данных. Возможности ruToken: ограниченное количество попыток ввода PIN-кода; интеграция в smartcard-ориентированное программное обеспечение; три уровня (гость, пользователь, администратор) доступа к токену. Цена - 770 р.
- eToken PASS. Идентификатор позволяет добавить поддержку аутентификации по одноразовым паролям в различные приложения. Возможности: не требуется установка дополнительного программного обеспечения; не требуется установка драйверов; функционирование с мобильных устройств; одноразовый односеансовый пароль. Цена - 850 р.
- eTokenPROAnywhere является электронным USB-ключом, позволяющий безопасно обращаться к Web-ресурсам. Возможности: открытие браузера и перенаправление пользователя только на заданные веб-сайты (адреса хранятся в защищённой памяти ключа); аутентификация пользователя; обеспечение защиты передаваемых по сети данных; защита от фишинга. Цена - 1032 р.

Рассмотрим применение метода анализа иерархии для решения поставленной задачи. Вначале требуется построение иерархической структуры: цель, критерии, альтернативы (таблица 1).

Таблица 1 - Иерархическая структура

Цель	Выбор наилучшего средства аутентификации				
Альтернативы	ruToken	eToken PASS	eTokenPro	eToken PRO Anywhere	iButton
Критерии	Цена	Возможности			Применяемость

Далее требуется провести сравнения альтернатив по каждому из трех показателей.

Рисунок 3. Сравнение выбранных идентификаторов относительно критерия "Цена"

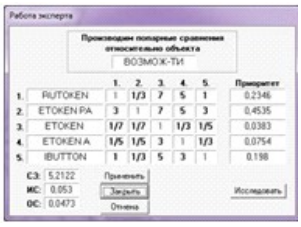


Рисунок 4. Сравнение выбранных идентификаторов относительно критерия "Возможности"

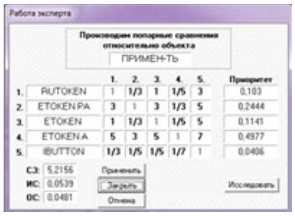


Рисунок 5. Сравнение выбранных идентификаторов относительно критерия "Применяемость"

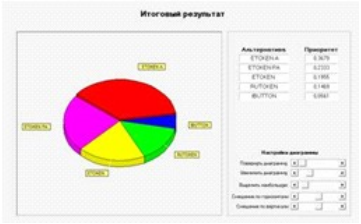


Рисунок 6. Результат сравнения идентификаторов по выбранным критериям

Таким образом, мы определили, что оптимальным средством аутентификации является идентификатор eToken PRO Anywhere, его значение глобального приоритета максимально - 0,3679.

Система защиты электронный замок "Соболь". Аппаратно-программный модуль доверенной загрузки "Соболь" позволяет защитить компьютеры от несанкционированного доступа и создавать замкнутую программную среду для работы пользователей. "Соболь" поможет предотвратить несанкционированную загрузку операционной системы как с внутренних носителей информации, так и съёмных, а механизм контроля целостности позволит отслеживать любые несанкционированные изменения в программной а аппаратной среде компьютера и запрещать работу на нём при их наличии.

Аппаратно-программный модуль может эффективно использоваться на предприятиях любого масштаба. Модуль применяется, когда необходимо предотвратить несанкционированный доступ к ресурсам защищаемого компьютера, разграничить доступ к информации и предотвратить несанкционированную её утечку при попытке обхода средств защиты.

Какие задачи решает:

- идентификация и аутентификация пользователей;
- контроль целостности аппаратной и программной среды компьютера;
- защита от несанкционированной загрузки ОС со съемных носителей;
- регистрация попыток доступа к компьютеру и иных событий безопасности;
- блокировка компьютера при попытке несанкционированного доступа или нарушении целостности программных или аппаратных компонентов;
- присутствует функция контроля работоспособности компонентов комплекса.

Внедрив "Соболь", заказчик сможет разграничить доступ пользователей к информации и компьютерам, предотвратить несанкционированную загрузку операционной системы со съемных носителей и последующую утечку информации, а механизм контроля целостности позволит контролировать неизменность программно-аппаратной среды компьютера.

Технические особенности

Электронный замок "Соболь" реализуется аппаратно-программным путём: он состоит из платы и программного обеспечения. "Соболь" может

применяться для защиты как автономных компьютеров, так и компьютеров и серверов, входящих в состав локальной вычислительной сети предприятия.

Программно-аппаратный модуль "Соболь" перехватывает момент загрузки операционной системы и продолжает её загрузку только после того, как пользователь предъявит свой идентификатор и будет проведена проверка целостности системы.

Контроль целостности имеет 2 режима функционирования:

- жесткий - запрет загрузки ОС и доступа к устройствам при нарушении целостности, регистрация факта нарушения целостности в журнале;
- мягкий - разрешение загрузки операционной системы и фиксация факта нарушения целостности в журнале.

Защита от несанкционированной загрузки операционной системы со съемных носителей реализуется путём блокировки доступа к устройствам чтения внешних носителей и USB-устройствам до момента загрузки штатной ОС, установленной на защищаемом компьютере. Доступ к устройствам восстанавливается при успешной загрузке штатной операционной системы, установленной на защищаемом компьютере.

Аппаратный датчик случайных чисел, входящий в состав модуля доверенной загрузки "Соболь" может применяться в СКЗИ для генерации надёжных ключей шифрования. Аппаратная часть комплекса исполняется в виде плат различных стандартов, начиная от PCI и заканчивая MINI-PCI-E. Электронный замок совместим с 64-битными версиями ОС Windows.

Электронный замок "Соболь" можно применять как автономное средство защиты, так и средство защиты, функционирующее в режиме совместного использования с другими решениями компании "Код безопасности".

При использовании "Соболя" совместно с другими решениями, часть функций управления "Соболем" передаётся на то средство защиты информации, совместно с которым он функционирует.

Основными этапами внедрения комплекса являются: установка программного обеспечения и платы, инициализация комплекса и его настройка. В результате внедрения заказчик получает дополнительный контроль над доступом сотрудников к ресурсам компьютеров и исключение несанкционированной загрузки операционной системы (как штатной, так и загружаемой со съемных носителей).

Система защиты информации Страж NT

Система защиты информации "Страж NT" (версия 3.0) предназначена для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа в многопользовательских автоматизированных системах на базе персональных ЭВМ. СЗИ "Страж NT" (версия 3.0) может применяться как на автономных рабочих местах, так и на рабочих станциях и серверах в составе локальной вычислительной сети. Отсутствие аппаратной составляющей позволяет применять СЗИ на компьютерах недесктопного исполнения (ноутбуки, сервера, промышленные компьютеры).

В СЗИ "Страж NT" (версия 3.0) реализованы следующие подсистемы и защитные механизмы:

- Строгая двухфакторная аутентификация до загрузки операционной системы с использованием аппаратных идентификаторов.
- Дискреционный и мандатный принципы разграничения доступа пользователей к ресурсам системы.
- Замкнутая программная среда для пользователей.
- Регистрация событий, в том числе и действий администратора.

- Маркировка печатных документов, независимо от приложения, выдающего их на печать.
- Гарантированное стирание освобождаемой оперативной памяти и удаляемых ресурсов системы.
- Контроль целостности критических ресурсов системы и компонентов системы защиты.
- Управление пользователями.
- Управление носителями информации.
- Преобразование информации на отчуждаемых носителях.
- Управление устройствами.
- Тестирование механизмов системы защиты.

"Страж NT" (версия 3.0) имеет сертификат ФСТЭК России, который позволяет использовать ее при создании автоматизированных систем до класса защищенности 1Б включительно и для защиты информации в ИСПДн до 1 класса включительно.

Обновленный 64-х разрядный релиз СЗИ "Страж NT" прошел летом 2012 года инспекционный контроль ФСТЭК России, подтвердивший соответствие СЗИ выданному ранее сертификату №2145. В обновленном релизе СЗИ "Страж NT" добавлена поддержка 64-х разрядных операционных систем MicrosoftWindows XP, WindowsServer 2003, WindowsVista, WindowsServer 2008, Windows 7 и WindowsServer 2008 R2.

Программно-аппаратная система защиты информации SecretNetявляется сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие требованиям регулирующих документов:

- №98-ФЗ ("О коммерческой тайне")
- №152-ФЗ ("О персональных данных")

- №5485-1-ФЗ ("О государственной тайне")
- СТО БР (Стандарт Банка России)

Сертификаты ФСТЭКРоссии позволяют использовать СЗИ от НСД SecretNet для защиты:

- конфиденциальной информации и государственной тайны в автоматизированных системах до класса 1Б включительно;
- информационных систем персональных данных до класса К1 включительно.

Расширен список операционных систем, добавлена поддержка 64-битных платформ.

Упрощен аудит безопасности за счет реализации возможности групповых операций с журналами. В программе управления отображаются зарегистрированные журналы от нескольких компьютеров по различным критериям событий безопасности.

Улучшена информативность программы оперативного управления ("Монитор") - реализована возможность отображения состояния защитных подсистем на клиентских рабочих станциях.

Добавлена поддержка персональных идентификаторов Rutoken, USB-ключи eToken PRO (Java), смарт-карты eToken PRO (Java), смарт-карты eToken PRO.

Исключено шифрование данных.

Возможности SecretNet 6:

- Аутентификация пользователей.
- Обеспечение разграничения доступа к защищаемой информации и устройствам.
- Доверенная информационная среда.
- Контроль каналов распространения конфиденциальной

информации.

- Контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации.
- Централизованное управление политиками безопасности, позволяет оперативно реагировать на события НСД.
- Оперативный мониторинг и аудит безопасности.
- Масштабируемая система защиты, возможность применения SecretNet (сетевой вариант) в организации с большим количеством филиалов.

Варианты развертывания SecretNet 6:

Автономный режим - предназначен для защиты небольшого количества (до 20-25) рабочих станций и серверов. При этом каждая машина администрируется локально.

Сетевой режим (с централизованным управлением) - предназначен для развертывания в доменной сети с ActiveDirectory. Данный вариант имеет средства централизованного управления и позволяет применить политики безопасности в масштабах организации. Сетевой вариант SecretNet может быть успешно развернут в сложной доменной сети (domaintree/forest).

Программное СЗИ "Электронный замок "eLock" предназначено для защиты ресурсов персонального компьютера от НСД при загрузке. В СЗИ "eLock" реализованы следующие функции защиты:

- идентификация и аутентификация пользователя до загрузки операционной системы (ОС);
- проверка ключевой идентификационной информации, хранящейся на внешних носителях (модификации Floppy и USB);
- остановка загрузки ОС при неуспешной идентификации и/или аутентификации;

- блокировка компьютера после трех неуспешных попыток аутентификации;
- регистрация событий в журнале учета (тип, имя пользователя, дата и время возникновения события);
- контроль целостности исполняемых модулей СЗИ "eLock 3.0.5002.0" и блокировка загрузки компьютера в случае ее нарушения;
- поддержка полномочий привилегированных (супервизора, администратора) и обычных (до восьми) пользователей;
- изменение PIN-кода доступа к USB- ключам и PIN-кодов USB-ключей;
- реализация загрузки только с устройства жесткого диска и блокировка клавиатуры при загрузке ОС.

Подсистема регистрации предназначена для регистрации входов в СЗИ "eLock", регистрации идентификации и аутентификации пользователей, регистрации изменения личного пароля администратора и пользователя, регистрации случаев блокировки компьютера, регистрации действий администратора по редактированию списка пользователей и регистрации очистки журнала. При установке "eLock" записывается в постоянно запоминающее устройство персонального компьютера, где располагается его базовая система ввода-вывода (BIOS). Данной СЗИ от НСД состоит из модуля реализации функций защиты и интерфейса СЗИ "eLock", и модуля реализующего работу с флэш-памятью ПЭВМ (неверная установка СЗИ может повредить базовую систему ввода-вывода, что приведет к потере работоспособности ПЭВМ).

Система защиты информации "DallasLock" <http://dehack.ru/szi_nsd/prog_tech-prog_szi/dallas_lock/>

Система защиты информации от несанкционированного доступа(СЗИ

от НСД)DallasLock представляет собой программный комплекс для обеспечения безопасности хранения и обработки данных в ОС семейства Windows.

СЗИ от НСДDallasLock предназначается для:

- разграничения доступа к информационным ресурсам и подключаемым устройствам;
- аудита действий пользователей, санкционированных и без соответствующих прав;
- централизованного управления механизмами безопасности;
- приведения АС, ГИС и обработки ПДн в соответствие требованиям законодательства по защите информации.

Версии СЗИ от НСД Dallas Lock представляют собой линейку сертифицированных решений для использования при создании комплексной системы защиты в автоматизированных системах до класса 1Б включительно и в информационных системах персональных данных до 1-го уровня включительно.

СЗИ от НСД Dallas Lock является полностью программным средством с возможностью подключения аппаратных идентификаторов, что обеспечивает ей реализацию двухфакторной аутентификации, присущей системам с повышенной сложностью. В то же время аппаратная идентификация обязательной не является.

Возможна установка актуальных версий на персональных компьютерах, портативных и мобильных компьютерах (ноутбуках и планшетных ПК), серверах (файловых, контроллерах домена и терминального доступа), также поддерживает виртуальные среды (Приложение В).

Преимущества:

- Настройка параметров безопасности собственными механизмами, полностью независимыми от ОС.
- Быстрое внедрение и эффективное управление многоуровневой системой защиты для распределенных конфигураций информационных сетей.
- Совместимость с другими технологиями и продуктами по защите информации (антивирусами, межсетевыми экранами, VPN, криптопровайдерами, IDS/IPS) и прикладным ПО.
- Широкий набор дополнительного функционала(помимо базовых требований РД).
- Оптимальная совокупная стоимость владения - от первичного приобретения до внедрения и сопровождения.

Возможности:

Архитектура СЗИ от НСД Dallas Lock включает в себя основные и дополнительные подсистемы, в том числе с уникальным функционалом.

- Аутентификация и разграничение доступа.
- Двухфакторная авторизация по паролю заданной сложности и аппаратному идентификатору.
- Дискреционный и мандатный принципы разграничения прав пользователей на доступ к глобальным, локальным и сетевым ресурсам файловой системы и подключаемым устройствам. Организация замкнутой программной среды и дополнительные механизмы ее настройки.
- Регистрация и учет действий пользователей.
- Настройка аудита и ведение журналов регистрации событий.
- Возможность фильтрации записей, экспорт и архивирование.
- Добавление штампа на распечатываемые документы.
- Контроль целостности.

- Обеспечение контроля целостности файловой системы, программно-аппаратной среды и реестра.
- Блокировка загрузки компьютера при выявлении изменений.
- Очистка остаточной информации.
- Объединение и управление защищенными компьютерами с помощью модуля"Сервер безопасности".
- Объединение нескольких Серверов безопасности в единый Лес безопасности с помощью модуля "Менеджер серверов безопасности".
- Дополнительные подсистемы и механизмы.
- Механизм преобразования данных в файл-контейнер.
- Механизм прозрачного преобразования жесткого диска.
- Модуль доверенной загрузки ПК уровня загрузочной записи.
- Задание списка расширений файлов, работа с которыми будет блокирована.
- Использование собственной графической оболочки для организации рабочего стола с ярлыками только необходимых программ.
- Подсистема самодиагностики функционала с формированием отчета.
- Удаленное администрирование и др.

.5 Практическое применение методов и средств сетевой безопасности

Межсетевой экран (другие названия брандмауэр, фаервол) - это комплекс аппаратных и программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами (защитный барьер между компьютером и сетью, к которой он подключен).

Порт - это идентифицируемый определенным номером системный ресурс, выделяемый приложению, которое выполняется на некотором сетевом хосте (компьютер или другое сетевое устройство), для связи с приложениями, которые выполняются на других сетевых хостах (в том числе с другими приложениями на этом же хосте). Есть много тысяч таких портов и у каждого есть свой уникальный номер.

Наиболее часто используемыми портами во всемирной сети являются:

1. 80 - порт для загрузки web-страниц;
2. 110 - используется по умолчанию для загрузки электронной почты;
. 25 - используется по умолчанию для отправки электронной почты.

Суть брандмауэра в том, чтобы закрыть порты, которые не используются. В противном случае через них злоумышленник или вредоносная программа (вирус, троян) могут проникнуть в ПК.

Рисунок 7. Расположение сетевого экрана (Firewall) в сети.

Виды межсетевых экранов

Брандмауэры можно поделить на две простые категории: аппаратные и программные. Аппаратным фаерволом может быть маршрутизатор, который

находиться между ПК и сетью Интернет. В таком случае к нему можно подключить несколько компьютеров и все они будут защищены брандмауэром, который является частью маршрутизатора. Программный межсетевой экран - это специализированное ПО, которое пользователь устанавливает себе на компьютер.

Типичные возможности:

- фильтрация доступа к заведомо незащищенным службам;
- препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
- контроль доступа к узлам сети;
- может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
- регламентирование порядка доступа к сети;
- уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Следует отметить, что использование фаервола увеличивает время отклика и снижает пропускную способность, поскольку фильтрация происходит не мгновенно.

Проблемы, не решаемые фаерволом:

- Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, онне защищает узлы сети от проникновения через "люки" (backdoors) или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь - утечки данных;
- не защищает от загрузки пользователями вредоносных программ,

в том числе вирусов;

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, антивирусы. Обычно они подключаются к фаерволу и пропускают через себя соответствующую часть сетевого трафика, работая как прозрачный для прочих сетевых узлов прокси, или же получают с фаервола копию всех пересылаемых данных. Однако такой анализ требует значительных аппаратных ресурсов, поэтому обычно проводится на каждом узле сети самостоятельно.

Аппаратный межсетевой экран ALTELL NEO - защита корпоративной, локальной сети.NEO - российские аппаратные межсетевые экраны нового поколения, сертифицированные ФСТЭК на самые высокие классы защиты. Главная особенность этих устройств - сочетание возможностей фильтрации трафика с функциями построения защищенных каналов связи (VPN), обнаружения и предотвращения вторжений (IDS/IPS) и контент-фильтрации (антивирусы, веб- и спам-фильтры, контроль приложений), что обеспечивает полное соответствие современной концепции унифицированной защиты сети (UnifiedThreatManagement, UTM, шлюз безопасности).

Рисунок 8. Аппаратный межсетевой экран ALTELL NEO

Преимущества ALTELL NEO:

- Полное соответствие требованиям российского законодательства

в области ИБ (сертификаты ФСТЭК и ФСБ);

- Широкий модельный ряд (небольшие и средние организации/холдинги/ЦОДы);
- Богатые функциональные возможности (FW, VPN, IDPS, антивирусный шлюз, почтовый фильтр, веб-фильтр);
- Открытые цены, наилучшее соотношение Мбит/руб.;
- Низкая совокупная стоимость владения (у младших моделей - 0 рублей);
- Модульная архитектура аппаратной и программной составляющих (3 варианта системного ПО:FW, VPN, UTM, дополнительные модули и опции);
- Высокая производительность, быстрое шифрование ГОСТ 28147-89;
- Разнообразие интерфейсов: 1/10 GbE (RJ45, SFP, SFP+), E1/T1, QDR 40 GbE (InfiniBand);
- Контроль приложений в реальном времени (L7-filtering);
- Работа в конвергентных сетях (данные, голос, видео);
- Поддержка режима динамической маршрутизации (RIP, OSPF, BGP);
- Простое управление с использованием командной строки, полноценного веб-интерфейса и отдельной системы мониторинга и управления;
- Встроенный учет трафика;
- Бесплатная трехлетняя гарантия работоспособности устройства;
- Бесплатная годовая техническая поддержка;
- Автоматическое обновление в режиме PUSH;
- Возможно использование отечественного UEFI BIOS (сейчас

используется в NEO 100);

- Русскоязычная техническая поддержка, подробная документация (3060 страниц).

Широкий модельный ряд ALTELL NEO позволяет удовлетворить запросы любой организации: от небольшой компании или регионального филиала до штаб-квартиры крупного территориально-распределенного холдинга или центра обработки данных. Модельный ряд ALTELL NEO приложение Г.

Одним из преимуществ устройств ALTELL NEO является их универсальность. В зависимости от варианта системного ПО (FW, VPN, UTM) они могут использоваться как межсетевой экран, маршрутизатор, криптошлюз, антивирусный шлюз, система обнаружения вторжений или веб-фильтр, а также выполнять все эти функции одновременно в качестве унифицированного шлюза безопасности (с вариантом ПО UTM). Таким образом, защита компьютерных сетей может быть обеспечена с помощью одного устройства (приложение Д).

<http://www.altell.ru.images.1c-bitrix-cdn.ru/upload/medialibrary/04b/04b9e43b7282c9d60064dd7c4770066a.jpg?1393490655251520>Устройства ALTELL NEO обладают всеми необходимыми сертификатами для использования в качестве средства защиты информации.

Рисунок 9. Возможности ALTELL NEO

Возможности:

- Защита локальной сети от нежелательного трафика;
- Обеспечение дифференцированных политик доступа к сети Интернет;
- Защита корпоративной сети от спама и вредоносного ПО;
- Разделение доступа к сегментам корпоративной сети, выделение сегментов ИСПДн и DMZ;
- Обнаружение и предотвращение вторжений (защита компьютерных сетей от хакерских атак);
- Обеспечение стабильности приоритетных соединений независимо от остальной нагрузки;
- Учет трафика и протоколирование соединений;
- Балансировка нагрузки между несколькими провайдерами;
- Создание отказоустойчивых кластерных решений;
- Объединение локальных сетей филиалов в единую защищенную корпоративную сеть;
- Защищенное подключение удаленных и мобильных пользователей к корпоративной сети;

- Блокировка нежелательных протоколов прикладного уровня;
- Защита корпоративной сети от DoS-атак.

. Экономическая часть

.1 Организационно-экономическое обоснование

В связи с массовым внедрением компьютеров во все сферы деятельности человека объем информации, которая хранится в электронном виде, вырос в тысячи раз, а с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру не дает гарантии сохранности информационных ресурсов. Все больше появляется специализированных средств защиты информации, которые ориентированы на решение, как правило, только одной задачи обеспечения безопасности системы или в редких случаях, некоторого ограниченного набора задач. Так, организациям, чтобы оградить себя от "компьютерных" преступлений приходится реализовывать целый набор мер. Расширение применения современных информационных технологий делает возможным распространение различных злоупотреблений, связанных с использованием вычислительной техники.

В качестве межсетевого экрана для офиса "Мегафон" будут рассматриваться разработки следующих компаний-производителей аппаратных средств защиты периметра:

- IBM;
- D-link;
- Cisco.

В результате выбора среди продуктов от каждой фирмы можно выделить продукты D-link DFL-260, IBM Proventia Network IPS и Cisco 1801/K9. Стоит отметить, что в выборе участвовал показатель "Цена", потому что необходимо экономическое обоснование выбора того или иного

продукта. Данное значение этого показателя учитывается в итоговом подсчете преимуществ. С этой целью приводится сравнительная таблица по основным характеристикам 3-х отобранных МЭ приложение Е.

Круг возможных потребителей:

- Небольшие компании с локальной сетью;
- Учебные учреждения (школы, техникумы, институты);
- Небольшие офисы, магазины.

Для больших предприятий подходит межсетевой экран ALTELL NEO он был описан в главе практическое применение методов и средств сетевой безопасности. Так как офис "Мегафон" небольшой, рассмотрим сетевой экран D-link DFL-260.

Круг возможных конкурентов:

- IBM ProventiaNetwork IPS;
- Cisco 1801/K9.

.2 Расчет себестоимости

Затраты на внедрение межсетевого экрана

Таблица 2. Затраты на оборудование

Наименование затрат	Ед.изм.	Количество	Цена	Сумма
Компьютер Dell с процессором Intel	шт.	10	10.250	102.500
межсетевой экран D-link DFL-260	Шт.	1	22.000	22.000
D -link лицензия	Мес.	12	5.000	5.000
Интернет	мес	5	350	1.750

Расчет заработной платы

Таблица 3. Расчет заработной платы

Начисления на зп	% отчислений
1. Пенсионный фонд - страховая часть	16%
2.Накопительная часть	6%
3.Фонд социального страхования	2,9%
4.фонд медицинского обязательно страхования	5,1%

Таблица 4. Заработная плата

Должность	Оклад	Кол-во отработанных дней	Премия	Отчисления на социальные фонды 30%	Всего начислено
Администратор безопасности 1.Январь 2.февраль 3.март 4.Апрель 5.Май	23000	13 17 18 20 14	10.000 15.000 14.000 18.000 9.300	9.900 11.400 11.100 12.300 9.690	23.100 26.600 25.900 28.700 22.610
Лаборант-помощник 1.Январь 2.февраль 3.март 4.Апрель 5.Май	10000	15 18 20 17 15	6.000 10.000 11.400 8.500 7.300	4.800 6.000 6.420 5.550 5.190	11.200 14.000 14.980 12.950 12.110

.3 Трудоемкость производства

Таблица 5. Расчет трудоемкости

Наименование этапа	Трудоемкость в днях
1.Разработка технического задания	3
2.подготовительный этап: - сбор информации; - выбор объективного построения программы; - разработка общей методики создания продукта	1 1 2
3.Основные этапы: - разработка основного алгоритма; - проверка.	2 2
4. Завершающий этап: - подготовка технической документации (сертификат); - сдача продукта.	3 2

3.4 Экономическая эффективность

Предполагаемая прибыль от межсетевого экрана D-link DFL-260 за 5 месяцев = 880.000, с лицензией 1080000.

Таблица 6. Расчет прибыли от МЭ за 5 месяцев

Месяц	Продано МЭ, шт.	Лицензия на 12 мес.	Цена МЭ	Сумма
Январь	4	5.000	22.000	108.000
Февраль	8	5.000	22.000	216.000
Март	7	5.000	22.000	189.000
Апрель	10	5.000	22.000	270.000
Май	11	5.000	22.000	297.000
Итого: 1080000				

Таблица 7. Расчет затрат за 5 месяцев

Наименование затрат	Сумма
Компьютер Dell с процессором Intel	102.500
межсетевой экран D-link DFL-260	22.000
D -link лицензия	5.000
Интернет	1.750
ЗП Администратор безопасности	181.000
ЗП Лаборант-помощник	93.200
Итого: 405.450	

Предполагаемая прибыль: = доход - затраты = Предполагаемая прибыль

ПП:= 1080000 - 405.450 = 674.550

Вывод

Внедрение продукта межсетевой экран актуально на сегодняшний день, так как даже самая маленькая организация должна быть защищена от НСД. Межсетевые экраны является выгодным продуктом для защиты организаций.

Распространение компьютерных систем и объединение их в коммуникационные сети усиливает возможности электронного проникновения в них. Во всех странах мира существует проблема компьютерной преступности, что вызывает необходимость привлечения все большего внимания и сил для организации борьбы с данным видом преступлений.

Возможности D-link DFL-260:

- Мощная система предотвращения атак (IPS);
- Фильтрация Web-содержимого;
- Профессиональная система предотвращения вторжений (IPS);
- Антивирусная (AV) проверка в реальном времени;
- Быстрая и эффективная фильтрация web-содержимого.
- Защита локальной сети от нежелательного трафика;
- Обеспечение дифференцированных политик доступа к сети Интернет;
- Защита корпоративной сети от спама и вредоносного ПО;

Заключение

Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированных доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте.

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются:

- переход от традиционной "бумажной" технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;
- объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;
- увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличением числа уязвимостей.

Компьютерные сети, в силу своей специфики, просто не смогут нормально функционировать и развиваться, игнорируя проблемы защиты информации.

В первой главе работы были рассмотрены различные виды угроз и рисков. Угрозы безопасности делятся не естественные и искусственные, а искусственные в свою очередь делятся на непреднамеренные и преднамеренные.

К самым распространенным угрозам относятся ошибки пользователей компьютерной сети, внутренние отказы сети или поддерживающей ее

инфраструктуры, программные атаки и вредоносное программное обеспечение.

Меры обеспечения безопасности компьютерных сетей подразделяются на: правовые (законодательные), морально-этические, организационные (административные), физические, технические (аппаратно-программные).

Для защиты локальной или корпоративной сети от атак из глобальной сети применяют специализированные программные средства: брэндмауэры или прокси-серверы. Брэндмауэры - это специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Прокси-сервер - это сервер-посредник, все обращения из локальной сети в глобальную происходят через него.

Для защиты корпоративной сети во второй главе рассмотрен Аппаратный межсетевой экран ALTELL NEO. Широкий модельный ряд ALTELL NEO позволяет удовлетворить запросы любой организации: от небольшой компании или регионального филиала до штаб-квартиры крупного территориально-распределенного холдинга или центра обработки данных.

Список используемых источников

1. Баженов Р.И. Информационная безопасность и защита информации: практикум. Биробиджан: Изд-во ГОУВПО "ДВГСГА", 2011. 140 с.

2. Баженов Р.И. О методике преподавания метода анализа иерархий в курсе "Информационная безопасность и защита информации" // Современные научные исследования и инновации. 2014. №4 (36). С. 76.

. Бикмаева Е.В., Баженов Р.И. Об оптимальном выборе системы защиты информации от несанкционированного доступа // APRIORI. Серия: Естественные и технические науки. 2014. №6. С. 5.

. Затеса А.В. Использование метода анализа иерархий для выбора информационной системы // Экономика, статистика и информатика. Вестник УМО. 2010. №6. С. 164-167.

. Ирзаев Г.Х. Экспертный метод аудита безопасности информационных систем Вестник Дагестанского государственного технического университета. Технические науки. 2011. Т. 1. №20. С. 11-15.

. Комполь В.В., Шиганова В.В., Баженов Р.И. Выбор программной платформы интернет-магазина с помощью метода анализа иерархий // Nauka-Rastudent.ru. 2014. №11 (11). С. 36.

. Программные системы поддержки принятия оптимальных решений MPRIORITY 1.0. URL: http://www.tomakechoice.com/mpriority.html

. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993.

. Савченко И.О. Выбор программного обеспечения для моделирования бизнес-процессов методом анализа иерархий Журнал научных публикаций аспирантов и докторантов. 2013. №6 (84). С. 35-37.

10. Родичев Ю.А. Компьютерные сети: архитектура, технологии, защита: учеб. Пособие для вузов. - Самара: изд-во "Универс-групп", 2006. - 468 с. - ISBN 5-467-00067-5.

11. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. И доп. - М.: Радио и связь, 2001. - 376 с.: ил.

. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. - М.: Академия, 2006. - 430 с. - ISBN: 5-908916-87-8

. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие - М.: ИД "Форум", 2011. - 352 с.

. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. - М.: ИД "Форум": ИНФРА-М, 2008. - 416 с.: ил. - (Профессиональное образование).

. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД "Форум": ИНФРА-М, 2010. - 592 с.: ил.

. Ясенев В.Н. Информационная безопасность в экономических системах: Учебное пособие - Н. Новгород: Изд-во ННГУ, 2006 - 253.

17. Vexler V.A., Bazhenov R.I., Bazhenova N.G. Entity-relationship model of adult education in regional extended education system 2014. Т. 10. №20. С. 1-14.

18. Li B., Chang X. Application of Analytic Hierarchy Process in the Planning of Energy Supply Network for Electric Vehicles // Energy Procedia. 2011. Т. 12. С. 1083-1089.

Список сокращений

ИСПД - информационную систему персональных данных

КС - компьютерные сети

МАИ - метод анализа иерархий

МЭ - Межсетевой экран

НСД - Несанкционированный доступ

ОС - операционная система

ПК - персональный компьютер

ПО - программное обеспечение

РД - Руководящий документ

СЗИ - система защиты информации- Disk Operating System - дисковая операционная систем- redundant array of independent disks - избыточный массив независимых дисков

Глоссарий

№	Понятие	Значение
1	Злоумышленник	Человек, совершивший преступление с заранее обдуманным намерением; замысливший какой-либо дурной, преступный поступок.
2	КС	(вычислительная сеть, сеть передачи данных) - система связи компьютеров или вычислительного оборудования (серверы, маршрутизаторы и другое оборудование). Для передачи данных могут быть использованы различные физические явления <https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D0%BA%D0%B0>, как правило - различные виды электрических сигналов <https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB>, световых сигналов или электромагнитного излучения <https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D0%B8%D1%82%D0%BD%D0%BE%D0%B5_%D0%B8%D0%B7%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5>
3	НСД	Несанкционированный доступ - доступ к информации <https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F> в нарушение должностных полномочий <https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BB%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%BD%D1%8B%D0%B5_%D0%BB%D0%B8%D1%86%D0%B0> сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Также несанкционированным доступом в отдельных случаях называют получение доступа к информации лицом, имеющим право на доступ <https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0> к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.
4	СЗИ	это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.
5	IBM	один из крупнейших в мире производителей и поставщиков

		аппаратного <https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5> и программного обеспечения <https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5>, а также ИТ-сервисов и консалтинговых услуг.
6	RAID	Технология виртуализации данных, которая объединяет несколько дисков в логический элемент для избыточности и повышения производительности.

Приложения

Приложение А

Классификация угроз

Приложение Б

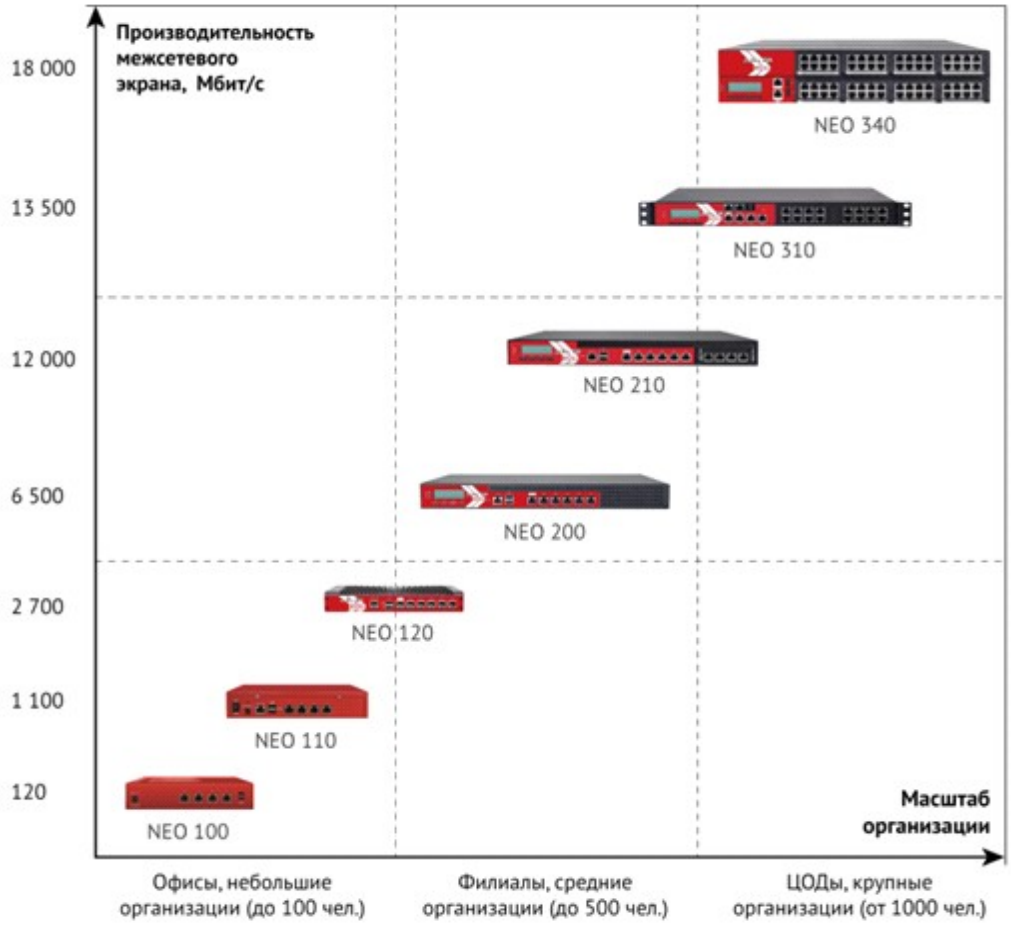
Классификация вирусов

Приложение В

Версия	Класс АС	Уровень ПДн	Класс ГИС	Централизованное управление	Поддерживаемые операционные системы	Поддерживаемые аппаратные идентификаторы	Сертификат соответствия
Dallas Lock 7.0	1В	1	1	Нет	Windows 2000/XP x32	iButton, USB-ключи и смарт-карта eToken	№ 896 от 06.05.2004 продлен до 11.05.2016
Dallas Lock 7.5	1Б	1	1	Есть	Windows 2000/XP/2003 x32	iButton, USB-ключи и смарт-карта eToken	№ 1685 от 18.09.2008 продлен до 18.09.2014
Dallas Lock 7.7	1Б	1	1	Есть	Windows XP/2003/Vista/2008/7 x32	iButton, USB-ключи и смарт-карта eToken, Рутокен	№ 2209 от 19.11.2010 продлен до 19.11.2016
Dallas Lock 8.0-К	1Г	1	1	Есть	Windows XP/2003/Vista/2008/7/2008 R2/8/2012/8.1/2012 R2 x32/x64	iButton, USB-ключи и смарт-карты eToken, USB-ключи Рутокен, USB-ключи и смарт-карты JaCarta, USB-Flash-накопители	№ 2720 от 25.09.2012 действителен до 25.09.2015
Dallas Lock 8.0-С	1Б	1	1	Есть	Windows XP/2003/Vista/2008/7/2008 R2/8/2012/8.1/2012 R2 x32/x64	iButton, USB-ключи и смарт-карты eToken, USB-ключи Рутокен, USB-ключи и смарт-карты JaCarta, USB-Flash-накопители	№ 2945 от 16.08.2013 действителен до 16.08.2016

Сертификаты соответствия DallasLock

Приложение Г



Модельный ряд ALTELL NEO

Приложение Д

Функции межсетевого экрана ALTELL NEO

Приложение Е

Результаты сравнительного анализа средств межсетевого экранирования

Характеристика	D-link DFL-260	IBM Proventia Network IPS	Cisco 1801/K9
Класс отказоустойчивости	1 класс	нет	1 класс
Контроль на прикладном уровне с учетом состояния	Нет	Да	Да
Контроль прикладного протокола	Да	Да	Да
Прозрачная аутентификация Windows	Да	Да	Да
Пропускная способность	80Mbps	10Mbps	100Mbps
Wi-Fi	Нет	Нет	Да
Интерфейсы	Ethernet 10/100BaseT (WAN) Ethernet 10/100BaseT (DMZ) 4 x Ethernet 10/100BaseT (ЛВС)	2 x Ethernet 10/100BaseT (WAN) Ethernet 10/100BaseT (DMZ) 8 x Ethernet 10/100BaseT (ЛВС)	ADSL (WAN)) 8 x Ethernet 10/100Ba (LAN) ISDN BRI
Протоколирование всех имен пользователей и приложений Web и Winsock	Да	Да	Нет
Поддержка Exchange	Да	Да	Да
Демилитаризованная зона	Да	Да	Нет
Контроль шлюзового и клиентского трафика VPN на прикладном уровне	Нет	Да	Да
Обнаружение и предотвращение несанкционированного доступа	Да	Да	Да
Сервер удаленного доступа VPN и шлюз VPN	Да	Да	Да
VPN-клиент	Да	Да	Да
100-Мбит/с порты ЛВС	4	8	8
Число одновременных подключений	12000	10000	18000
Передача функций отказавшего МЭ исправному устройству	Нет	Нет	Да
Переключение Интернет-провайдера и объединение полосы пропускания	Нет	Да	Нет
Конфигурирование Web-интерфейс	Да	Да	Да
Web-кэширование и proxy	Да	Нет	Да
Цена	22.000 руб.	150.000 руб.	36.000 руб.
Общее количество недостатков систем	3	4	3