ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

БАЙМИРЗАЕВ ИЛХОМ БАХРОМОВИЧ

Разработка методов и прикладных программ для ограничения доступа хостов внутри сети

5А330601-Программный инжиниринг

Диссертация
на соискание академической степени магистра

Научный руководитель
кандидат технических наук
Ахмедова О.П.

Ташкент – 2015

Содержание

Введение

Сегодня на приоритетные позиции в Республике Узбекистан выходят компьютерные и информационные технологии, развитие и модернизация сетей телекоммуникаций, передачи данных, доступа к услугам Интернет. Громадное распространение Интернета привело к тому, что сетевой стек протоколов TCP/IP стал практически основным при организации межсетевого взаимодействия. Разработанная в конце 70-х годов XX в. совокупность протоколов опиралась на уровневую структуру, которая послужила основой для последующих разработок модели OpenSystemInterconnection.

Технология данного стека протоколов оказалась настолько удобной, что ее стали использовать не только для работы в Интернете, но и при организации работы в корпоративных сетях.

Актуальность работы. Диссертационная работа посвящена исследованию методов и прикладных программ для ограничения доступа хостов внутри сети. Бурное развитие всемирных компьютерных сетей, разработка новейших систем поиска информации все больше привлекают внимание к сети Интернет со стороны как физических, так и юридических лиц. Большинство организаций принимает решения по внедрению своих локальных и корпоративных сетей в Интернет. Использование Интернета в коммерческих целях и при передаче конфиденциальной информации приводит к необходимости создания эффективной системы защиты данных. Развитие глобальных сетей ведет к быстрому увеличению количества не только пользователей, но и атак на компьютеры, подключенные к Интернету. Ежегодные потери из-за низкого уровня защиты компьютеров оцениваются десятками миллионов долларов. Именно поэтому при подключении к Интернету корпоративной или локальной сети важно не забыть позаботиться об обеспечении ее информационной безопасности. Сейчас вряд ли кому-либо нужно доказывать, что при подключении к Интернету риску подвергается

безопасность локальной сети и конфиденциальность содержащейся в ней информации. По данным CERT CoordinationCenter в 1995 году было зарегистрировано 2421 инцидентов - взломов локальных сетей и серверов. По результатам опроса, проведенного Computer Security Institute (CSI) среди 500 наиболее крупных организаций, компаний и университетов с 1991 число незаконных вторжений возросло на 48.9 %, а потери, вызванные этими атаками, оцениваются в 66 млн. долларов США.

Часть задач по отражению наиболее возможных угроз для внутренних сетей могут решать межсетевые экраны. Использование межсетевых экранов дает возможность организовать внутреннюю политику безопасности сети предприятия, поделив всю сеть на сегменты, и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение: дать ему возможность пройти или нет. Для того чтобы межсетевой экран смог осуществить эту операцию, ему нужно определить набор правил фильтрации. Решение о том, фильтровать ли с помощью межсетевого экрана конкретные протоколы и адреса, зависит от принятой в защищаемой сети политики безопасности. Межсетевой экран представляет собой набор компонентов, настраиваемых для реализации выбранной политики безопасности.

В последнее время тема использования межсетевых экранов становится актуальной, потому что все большее число людей и организаций становится жертвами компьютерных взломщиков. И, тем не менее, количество пользователей в сети не уменьшается, а наоборот растет с огромной прогрессией.

Объект и предмет исследования. Объектом исследования является компьютерные сети. Предметом исследования являются методы, алгоритмы и программные средства защиты информации.

Цели и задачи работы. Целью диссертационной работы является рассмотрение вопросов повышения эффективности прикладных программ для ограничения доступа хостов внутри сети.

Для достижения поставленной цели в магистерской диссертационной работе решаются следующие задачи:

- анализ требований к средствам защиты сетей
- анализ существующих средств ограничения доступа в компьютерной сети;
- анализ современных криптографических методов защиты информации
- разработка алгоритма для ограничения доступа;
- разработка средства защиты компьютерных сетей, работающего на прикладном уровне.

Гипотеза исследования. Возможность повышения защищенности компьютерных сетей за счет использования методов и алгоритмов ограничения доступа.

Краткий анализ литератур по теме. Исследованию теоретических и практических аспектов проблем обеспечения информационной безопасности, различным подходам к их решению посвящены многочисленные работы ученых, таких как В.А. Герасименко, А.А. Грушо, Д.П. Зегжда, LeonardJ. LaPadula, HarrisonM., RuzzoW., UhlmanJ., PhamH., Ф.Б. Абуталиева, Т.Ф. Бекмуратова, П.Ф. Хасанова, М.М. Арипова, З.Т. Адиловой, С.К. Ганиева, М.М. Каримова и многих других.

Методы исследования. Основными методами исследований являются: методы и средства защиты информации, объектно-ориентированное программирование.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в применении разных механизмов защиты

информации, позволяющие активно вести исследования в области обеспечения безопасности.

Практическая значимость заключается в применении программного обеспечения в защиты компьютерных сетей работающего на прикладном уровне для обеспечения функционирования различных сетевых служб.

Научная новизна работы. Научная новизна заключается в применении разработанного метода для повышения эффективности работы ограничения доступа хостов внутри сети.

Структура диссертационной работы. Диссертация состоит из введения, 3 глав, заключения, библиографического списка и приложения. Основной текст работы изложен на страницах и содержит таблицы и рисунков.

Глава 1. Анализ требований к средствам защиты сетей от несанкционированных воздействий

1. Угрозы информационной безопасности в современных компьютерных сетях

К настоящему времени известно большое количество разноплановых угроз различного происхождения, таящих в себе различную опасность для информации. Виды угроз - это основополагающий параметр, определяющий целевую направленность защиты информации.

Под случайным понимается такое происхождение угроз, которое обусловливается спонтанными и не зависящими от воли людей обстоятельствами, возникающими в системе обработки данных, а процессе ее функционирования.

Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния:

- отказ - нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций;
- сбой - временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;
- ошибка - неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций происходящее вследствие специфического (постоянного или временного) его состояния;
- побочное влияние - негативное воздействие на систему вцелом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или вовнешней среде.

Преднамеренное происхождение угрозы обусловливается злоумышленными действиями людей, осуществляемыми в целях реализации одного или нескольких видов угроз.

Отмечены две разновидности предпосылок появления угроз: объективные (количественная иди качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются следующим образом:

- количественная недостаточность - физическая нехватка одного или нескольких элементов системы обработки данных, вызывающая нарушения технологического процесса обработки и (или) перегрузку имеющихся элементов;
- качественная недостаточность - несовершенство конструкции (организации) элементом системы, ксилу чего могут появляться возможности для случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;
- деятельность разведывательных служб иностранных государств - специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами;
- промышленный шпионаж - негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или похищения, а также по созданию для себя благоприятных условий в целях получения максимальной выгоды;

– действия криминальных и хулиганствующих элементов - хищение информации или компьютерных программ в целях наживы или их разрушения в интересах конкурентов;
– злоумышленные действия недобросовестных сотрудников - хищение (копирование) или уничтожение информационных массивов и (или) программ по эгоистическим или корыстным мотивам.

Источниками угроз являются люди, технические устройства, программы и алгоритмы, технологические схемы обработки данных и внешняя среда:

– люди — персонал, пользователи и посторонние лица, которые могут взаимодействовать с ресурсами и данными организации непосредственнос рабочих мест и удаленно, используя сетевое взаимодействие;
– технические средства — непосредственно связанные с обработкой, хранением и передачей информации (например, средства регистрации данных, средства ввода и т.п..) и вспомогательные (например, средства электропитания, кондиционирования и т.д.);
– модели, алгоритмы и программы. Эту группу источников рассматривают как недостатки проектирования, реализации и конфигурации (эксплуатации) и называют недостатками программного обеспечения (общего назначения, прикладного и вспомогательного),
– технологическая схема обработки данных - выделяют ручные, интерактивные, внутримашинные и сетевые технологические схемы обработки;
– внешняя среда - выделяют состояние среды (возможность пожаров, землетрясений и т.п.), побочные шумы (особенно опасные при

передаче данных) и побочные сигналы (например, электромагнитное излучение аппаратуры).

Основными причинами утечки информации являются;

– несоблюдение персоналом норм, требований, правил эксплуатации;

– ошибки в проектировании системы и систем защиты;

– целение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований и эксплуатации может быть как умышленным, так и непреднамеренным.

От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации, и они бывают в трех видах:

– разглашение;
– несанкционированный доступ к информации;
– получение защищаемой информации разведками (как отечественными, так и иностранными).

Под разглашением информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Под несанкционированным доступом понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может бить Государство юридическое лицо, группа

физических лиц (в том числе общественная организация), отдельное физическое лицо.

Получение защищаемой информации разведкам и может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

Канал утечки информации - совокупность источника информации, материального носителя или среды распространении несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может располагаться в пределах контролируемой зоны, охватывающей систему или вне нее.

2. Современные средства защиты от несанкционированного копирования

Защита программного обеспечения— комплекс мер, направленных на защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов.

Защита от несанкционированного использования программ — система мер, направленных на противодействие нелегальному использованию программного обеспечения. При защите могут применяться организационные, юридические, программные и программно-аппаратные средства.

Защита от копирования к программному обеспечению применяется редко, в связи с необходимостью его распространения и установки на компьютеры пользователей. Однако, от копирования может защищаться

лицензия на приложение (при распространении на физическом носителе) или его отдельные алгоритмы.

Технические средства защиты. Методы можно классифицировать по способу распространения защищаемого программного обеспечения и типу носителя лицензии.

Локальная программная защита. Требование ввода серийного номера (ключа) при установке/запуске. История этого метода началась тогда, когда приложения распространялись только на физических носителях (к примеру, компакт-дисках). На коробке с диском был напечатан серийный номер, подходящий только к данной копии программы.

С распространением сетей очевидным недостатком стала проблема распространения образов дисков и серийных номеров по сети. Поэтому в настоящий момент метод используется только в совокупности одним или более других методов (к примеру, организационных).

Протокол(protocol) — описание распределенного алгоритма, в процессе выполнения которого два (или более) участника последовательно выполняют определенные действия и обмениваются сообщениями. Последовательность шагов протокола группируется в циклы (раунды). В качестве участников (иначе — субъектов, сторон) протокола могут выступать не только пользователи или абоненты, но и процессы, выполняющие какую-либо функциональную роль, например клиентские и серверные приложения. Предполагается, что все участники выполняют в нем какую-либо активную роль, а пассивные наблюдатели не являются участниками протокола.

Цикл (раунд) протокола(round, passofcryptographicprotocol) — в криптографических протоколах с двумя участниками — временной интервал, в котором активен только один из участников. Другое название — *проход*(pass) *протокола*. Цикл (раунд) завершается формированием и отправлением сообщения с последующим переходом активного участника в

состояние ожидания и передачей активности другому участнику. В протоколах с тремя и более участниками в синхронном случае цикл — период времени между двумя точками синхронизации. К очередной точке синхронизации каждый участник должен отправить все сообщения, которые ему предписано передать другим участникам в текущем цикле.

Шаг протокола(stepofaprotocol, protocolaction) — конкретное законченное действие, выполняемое участником протокола во время одного цикла (раунда) протокола; например, вычисление значения некоторой функции, проверка правильности сертификата ключа, генерация случайного числа, отправка сообщения и т. п.

Коммуникационный протокол устанавливает последовательность действий участников при передаче информации или информационном обмене. Обычный коммуникационный протокол обеспечивает установку соединения/сеанса, выбор маршрута, обнаружение искажений, восстановление передаваемой информации и т. п.

3. Применение средств защиты в современных корпоративных сетях

Функция — сервис безопасности(security services) — защитная функция, выполняемая подсистемой безопасности и определяемая ее целевым назначением. В соответствии со стандартом ISO7498.2 выделено пять классов таких функций для архитектуры безопасности эталонной модели взаимодействия: аутентификация сторон и аутентификация источника данных, разграничение доступа, конфиденциальность, целостность данных и невозможность отказа от факта отправления или получения сообщения, которые могут конкретизироваться для конкретных условий применения (табл. 1).

Для построения защищенных распределенных систем современные стандарты определяют и ряд других функций — сервисов безопасности,

например туннелирование, межсетевое экранирование, сокрытие трафика и др.

Обычно используют следующее расположение сервисов для создания «эшелонированной обороны» в общей архитектуре информационной системы:

- средства выявления злоумышленной активности и контроля защищенности;
- межсетевое экранирование для защиты внешних соединений и поддержка виртуальных частных сетей (периметр безопасности);
- активный аудит и управление (для обнаружения атак);
- идентификация/аутентификация и управление доступом;
- конфиденциальность;

Таблица 1.

Функции — сервисы безопасности

Функция — сервис безопасности	**Назначение функции**
Аутентификация источникаданных(dataoriginauthentication service)	Обеспечивает возможность проверки того, что полученные данные действительно созданы конкретным источником. Данная функция не обеспечивает защиты от повторного навязывания или модификации данных
Аутентификациясторон(peer entity authentication service)	Обеспечивает возможность проверки того, что одна из сторон информационного взаимодействия действительно является той, за которую себя выдает. Применяется в целях защиты от атаки типа имитация и от атаки на протокол с повторной передачей
Конфиденциальностьданных(data confidentiality service)	Обеспечивает невозможность несанкционированного получения доступа к данным или раскрытия данных

Невозможность отказа (non- repudiation service)	Обеспечивает невозможность отказа одной из сторон от факта участия в информационном обмене (полностью или в какой-либо его части)
Невозможность отказа с доказательством получения (non-repudiation service with proof of delivery)	Обеспечивает невозможность отказа получателя от факта получения сообщения
Невозможность отказа с доказательством источника (non-repudiationservicewithproofoforigin)	Обеспечивает невозможность отказа одной из сторон от факта отправления сообщения
Целостностьданных(data integrity service)	Обеспечивает возможность проверки того, что защищаемая информация не подверглась несанкционированной модификации или разрушению
Функция — сервис безопасности	Назначение функции
Обеспечение целостности соединения без восстановления (connectionintegrityservicewithoutrecovery)	Обеспечивает возможность проверки того, что все данные, передаваемые при установленном соединении, не подверглись модификации без восстановления этих данных
Обеспечение целостности соединения с восстановлением (connectionintegrityservicewithrecovery)	Обеспечивает возможность проверки того, что все данные, передаваемые при установленном соединении, не подверглись модификации с восстановлением этих данных
Разграничениедоступа (access control service)	Обеспечивает невозможность несанкционированного использования ресурсов системы. Данный термин

	понимается в самом широком смысле. На практике решение о предоставлении доступа основывается на аутентификации сторон

Понятие криптографического протокола. Возвращаясь к протоколам, заметим, что фактически большинство основных свойств безопасности реально обеспечивается только криптографическими методами и за их выполнение отвечает криптографическая подсистема. Поэтому защищенные протоколы часто отождествляют с криптографическими протоколами.

Криптографический протокол(cryptographicprotocol) — протокол, предназначенный для выполнения функций криптографической системы; в процессе его выполнения участники используют криптографические алгоритмы. В данном случае под *криптографической.системой* понимают систему обеспечения безопасности информации криптографическими методами. В настоящее время основными функциями криптографической системы являются обеспечение конфиденциальности, целостности, аутентификации, невозможности отказа и неотслеживаемости. В качестве подсистем она может включать системы шифрования, системы идентификации, системы имитозащиты, системы цифровой подписи и некоторые другие, а также ключевую систему, обеспечивающую работу остальных систем.

В основе выбора и построения криптографических систем лежит условие обеспечения криптографической стойкости. Под *стойкостью* криптографических систем понимают их способность противостоять атакам противника и (или) нарушителя, как правило, имеющим целью нейтрализацию одной или нескольких функций безопасности и, прежде всего, получение секретного ключа. Под *нарушителем* в данном случае понимается внутренний нарушитель, т.е. участник протокола, нарушающий предписанные протоколом действия, а под *противником* — внешний субъект

(или коалиция субъектов), наблюдающий за передаваемыми сообщениями и, возможно, вмешивающийся в работу участников путем перехвата, искажения (модификации), вставки (создания новых), повтора и перенаправления сообщений, блокирования передачи в целях нарушения одной или нескольких функций — сервисов безопасности. Часто допускается, что противник может образовывать коалицию с нарушителем. Заметим, что во многих формальных методах анализа протоколов противник отождествляется с сетью (точнее — с совокупностью каналов связи), по которой проводится обмен сообщениями.

Межсетевым экраном называют специализированный программный комплекс, используемый для защиты определенных частей компьютерной сети компании. Применяя межсетевой экран, можно разделить компьютерную сеть на две части и указать правила фильтрации пакетов информации при переходе из одной части в другую. В основном эта граница проводится между корпоративной сетью компании и сетью Интернет. Межсетевой экран также называют брандмауэром или файрволом (firewall). Исторически применение файрволов стало одним из первых методов защиты корпоративных сетей компаний. Сейчас установка сетевого экрана является одним из основополагающих правил защиты сети [7].

Для реализации функций контроля межсетевого доступа межсетевой экран должен располагаться между защищаемой сетью компании и потенциально опасной внешней сетью. При этом все функции по передаче информации между этими сетями должны реализовываться только через него. Межсетевой экран дает возможность решить, как правило, две основных задачи:

- контроль и ограничение доступа из внешних источников к внутренним ресурсам сети. Ограничение доступа имеет значение при подключении к корпоративной сети предприятия клиентов и

партнеров, а также при попытках несанкционированного доступа со стороны злоумышленников.

– контроль доступа пользователей внутренней сети к внешним ресурсам данных.

Как правило, это ресурсы, не имеющие прямого отношения к выполнению сотрудниками служебных функций. Межсетевой экран способен выполнять довольно много разнообразных функций по обеспечению информационной безопасности. В основном, его функционал зависит от поставленных перед ним администратором сети задач. Фильтрация трафика. Смысл фильтрации потоков информации состоит в выборочном пропускании через брандмауэр случайных пакетов данных. Идентификация потенциально опасной информации основывается на загружаемых в межсетевой экран правилах, которые, в свою очередь, определяются политикой безопасности, принятой в данной организации.

Правила, загружаемые в межсетевой экран, обозначают как набор фильтров, каждый из которых отвечает за определенный критерий отбора. Функции, применяемые для фильтрации трафика, – определение какие пакеты данных могут быть пропущены во внутреннюю сеть, а какие нет, при помощи межсетевого экрана с тем же успехом используются и для определения уровня доступа пользователей сети. Прежде чем дать пользователю возможность доступа к определенному ресурсу, брандмауэр сначала проводит его аутентификацию (как правило, ввод логина/пароля), затем, на основании полученных данных, авторизацию (определение прав доступа) и, сопоставляя, права доступа к ресурсу и права доступа пользователя дает возможность воспользоваться ресурсом или запрещает его использование.

Существует мнение, что маршрутизатор также может играть роль межсетевого экрана. Однако между этими устройствами существует одно принципиальное различие: маршрутизатор предназначен для быстрой

маршрутизации трафика, а не для его блокировки. Межсетевой экран представляет собой средство защиты, которое пропускает определенный трафик из потока данных, а маршрутизатор является сетевым устройством, которое можно настроить на блокировку определенного трафика.

Кроме того, межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу.

Название «брандмауэр», казалось бы, относится к одному устройству или одной программе. Но во всех случаях, за исключением простейших, лучше представлять себе его как ***систему компонентов,*** предназначенных для управления доступом к вашей и внешней сетям на основе определенной политики безопасности. Термин «межсетевой экран» был принят для обозначения совокупности компонентов, которые находятся между вашей сетью и внешним миром и образуют защитный барьер.

В результате конкуренции среди производителей межсетевых экранов и их попыток усовершенствовать свой продукт брандмауэры наделялись новыми свойствами. Поскольку межсетевой экран стоит на границе вашей сети и служит как бы воротами во внешний мир, он должен выполнять множество задач, в том числе и не связанных с обеспечением безопасности. Вот некоторые из новых функций, которые имеются в современных брандмауэрах:

- ***кэширование*** (caching). Это свойство особенно характерно для сетей, содержащих Web-серверы с большим объемом информации, доступной изИнтернет. Благодаря локальному хранению часто запрашиваемых данных кэширующий сервер может улучшить время реакции на запрос пользователя и сэкономить полосу пропускания, которая потребовалась бы для повторной загрузки данных;
- ***трансляция адреса*** (addresstranslation). Настроенный соответствующим образом брандмауэр позволяет применять для внутренней сети любые IP-адреса. При этом снаружи виден только адрес брандмауэра;
- ***фильтрация контента*** (contentrestriction). Все большее число продуктов обеспечивает ограничение информации, получаемой пользователями из Internet, путем блокирования доступа к адресам URL, содержащим нежелательный контент, или поиска заданных ключевых слов в приходящих пакетах данных;
- ***переадресация*** (addressvectoring). Эта функция предоставляет брандмауэру возможность изменять, например, запросы HTTP так, чтобы они направлялись серверу не с указанным в пакете запроса IP-адресом, а с другим. Таким способом удается распределять нагрузку между несколькими серверами, которые для внешнего пользователя выглядят как одиночный сервер.

4.Криптографические методы защиты информации

Без использования криптографии сегодня немыслимо решение задач по обеспечению безопасности информации, связанных с конфиденциальностью и целостностью, аутентификацией и невозможностью отказа от авторства. В наши дни использование криптографических методов получило широкое распространение благодаря развитию компьютерных сетей и электронного

обмена данными в различных областях: финансах, банковском деле, торговле и т. д.

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных[5].

В настоящее время существуют 4 вида криптосистем.

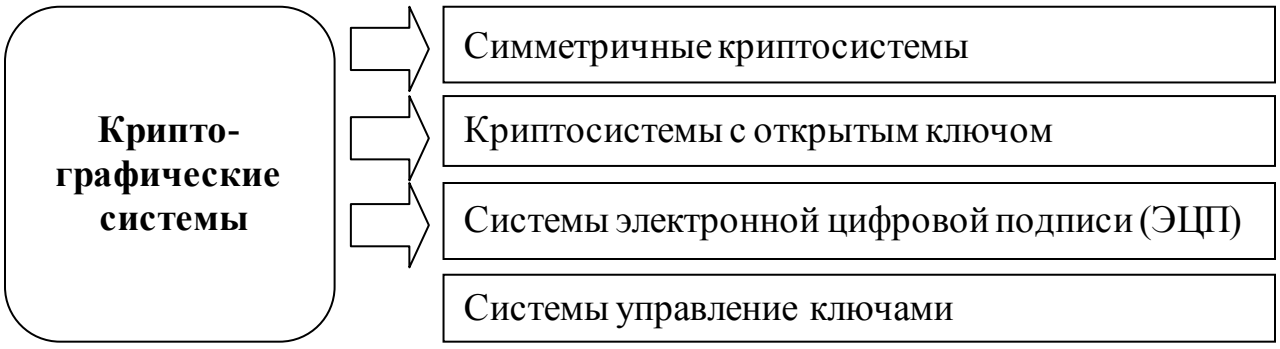

Рис.1. Виды современных криптосистем

Криптографическая система, в которой один и тот же криптографический ключ используется для шифрования и дешифрования информациинаызываются симметричными.

Криптографическая система, в которой используются два ключа - ссекретный и открытый, называются асимметричными.Причем ни один из ключей не может быть вычислен из другого за приемлемое время. Секретный ключ должен содержаться в тайне, в то время как открытый ключ может быть разослан всем абонентам, с которыми осуществляется взаимодействие.

Для обеспечения безопасности данных необходимо поддерживать три основные функции:

- защиту конфиденциальности передаваемых или хранимых в памяти данных;

- подтверждение целостности и подлинности данных;

- аутентификацию абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легальность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Обеспечение конфиденциальности, целостности и подлинности передаваемых и сохраняемых данных осуществляется прежде всего правильным использованием криптографических способов и средств защиты информации. Основой большинства криптографических средств защиты информации является *шифрование данных*.

В соответствии с выполняемыми задачами по защите информации можно выделить два основных класса криптографических систем:

- криптосистемы, обеспечивающие секретность информации;

-криптосистемы, обеспечивающие подлинность (аутентичность) информации.

Такое разделение обусловлено тем, что задача защиты секретности информации (сохранения ее в тайне) принципиально отличается от задачи защиты подлинности (аутентичности) информации, а поэтому должна решаться другими криптографическими методами.

Общая классификация криптосистем в соответствии с выполняемыми ими задачами по защите информации представлена на рис. 2. Криптосистемы, обеспечивающие секретность информации, разделяются на системы шифрования и системы криптографического кодирования информации [21].

Системы шифрования информации исторически являются самыми первыми криптографическими системами.

В общем случае шифрование сообщения (информации) есть обратимое преобразование сообщения, не зависящее от самого сообщения, с целью скрытия его содержания. Зашифрованное сообщение называется шифрограммой. Преобразование сообщения в шифрограмму описывается функцией шифрования; преобразование шифрограммы в сообщение описывается функцией дешифрования.

Другим методом обеспечения секретности информации является криптографическое кодирование. Криптографическое кодирование информации есть в общем случае преобразование по ключу сообщений в кодограммы, зависящее от самих сообщений, с целью скрытия их содержания. Системами криптографического кодирования информации называются криптографические системы, в которых защита информации по ключу основана на использовании ее избыточности. Криптосистемы аутентификации информации предназначены для контроля ее подлинности,

но в ряде случаев они способны эффективно обеспечить контроль целостности сообщений при различных деструктивных воздействиях.

Данный класс криптосистем может быть разделен в зависимости от решаемой задачи на системы аутентификации информации (сообщений) и системы аутентификации источников информации (корреспондентов, пользователей, сетей, систем и т. п.). Методы аутентификации информации различаются в зависимости от условий обеспечения подлинности информации.

Рис.2. Классификация криптографических систем защиты информации.

Подлинность информации в условиях взаимного недоверия сторон может быть обеспечена с использованием так называемой электронной

цифровой подписи сообщения, формируемой отправителем и проверяемой получателем сообщений. Невозможность выполнения каких-либо действий отправителя за получателя и получателя за отправителя при использовании цифровой подписи сообщения обусловлена тем, что они для формирования и проверки цифровой подписи используют различную ключевую информацию. Большинство криптографических систем и протоколов аутентификации объектов построены на основе криптосистем цифровой подписи сообщений.

Криптосистемы, обеспечивающие доступность информации, в настоящее время не являются самостоятельным классом и строятся на основе принципов, заимствованных из криптосистем аутентификации информации и криптосистем обеспечения секретности информации.

Выводы по первой главе

1. Анализ угроз информационной безопасности в современных компьютерных сетях показали отмеченные две разновидности предпосылок появления угроз: объективные и субъективные. Количественная или качественная недостаточность элементов системыдеятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы и .т.д.
2. Анализ ссовременных средств защиты от несанкционированного копирования показали что безопасность протокола выражается в обеспечении гарантий выполнения таких свойств, характеризующих безопасность, как доступность, конфиденциальность, целостность и др. Для обеспечения функций безопасности, отвечающих этим свойствам, в протоколах применяют специальные конструкции. Протокол, обеспечивающий поддержку хотя бы одной из функций безопасности,

называют защищенным, или, точнее, протоколом обеспечения безопасности (security protocol).

3. Все функциональные возможности дают определенные преимущества в плане гарантий безопасности, но в основном предназначены для увеличения производительности. Например, в результате переадресации и трансляции адреса удается скрыть внутренние IP-адреса от хакеров, что безусловно повышает безопасность. Чем меньшей информацией располагает потенциальный нарушитель, тем более сложной будет его работа. Но эти же возможности служат администратору при распределении нагрузки среди нескольких компьютеров. Благодаря трансляции адреса вам не понадобится запрашивать большой диапазон адресов IP для всех серверов и рабочих станций в вашей сети.

4. Краткое рассмотрение возможных методов защиты информации свидетельствует о том, что многие задачи защиты информации наиболее эффективно решаются криптографическими методами, а ряд задач вообще может быть решен только с использованием криптографических методов защиты информации.

Глава II. Анализ существующих методов и средств ограничения доступа

1. Анализ существующих методов ограничения доступа

Основные протоколы

Передача ключей с использованием симметричного шифрования. Протоколы распределения ключей отличаются как по назначению, так и по способам реализации. Можно выделить три типа протоколов распределения ключей:

- Протоколы передачи (ранее сгенерированных) ключей (обмена ключами);
- Протоколы совместной выработки общего ключа (открытое распределение ключей);
- Схемы предварительного распределения ключей.

Различают также протоколы распределения ключей междуотдельными участниками и между группами участников информационного взаимодействия.

Двусторонние протоколы. Рассмотрим сначала двусторонние протоколы передачи ключей с использованием симметричного шифрования. Различают протоколы, в которых стороны заранее располагают какой-либо известной им обеим секретной информацией, и протоколы, не требующие этого условия.

Пусть стороны Aи B заранее обладают общей секретной информацией. Допустим, что это — секретный ключ k_{ab}, тогда для передачи ключаkстороны могут использовать одностороннею передачу:

$A \longrightarrow B: Ek_{AB}(k,t,B)$

где E — алгоритм шифрования;t— метка времени; B — идентификатор участника B.

Подчеркнем, что если не передавать метки времени, то злоумышленник может осуществить повторную передачу того» же сообщения. Если же не указывать идентификатор адресата, то злоумышленник может вернуть отправителю перехваченное сообщение, что в некоторых ситуациях может быть опасным, поскольку абонент A не сможет установить, что это сообщение получено не от абонента B. Заметим также, что временная метка и идентификатор могут служить дополнительным подтверждением правильности источника, так как соответствие форматов этих полей после их расшифрования принятым в системе свидетельствует о том, что зашифрование мог осуществить только абонент A.

Заметим, что в приведенном протоколе вместо шифрования можно использовать ключевую хеш-функцию, зависящую от общего ключа:

$A \rightarrow B: k \oplus h_{kAB}(t, B)$.

Правда, здесь теряется возможность проверки правильности формата и тем самым подтверждение правильности получения ключа можно будет осуществить только после дополнительного обмена сообщениями.

Если предъявить к протоколу требование проведения аутентификации сеанса в целях более надежной аутентификации источника и подтверждения единственности и своевременности передачи сообщений для защиты от повторной передачи, то можно использовать следующий протокол типа «запрос-ответ»:

1. $A \leftarrow B: r_B$;
2. $A \rightarrow B: E_{kAB}(k, r_B, B)$,

где r_B — случайное число, сгенерированное участником B и переданное участнику A в начале сеанса.

При использовании хеш-функции подобный протокол может выглядеть так:

1. $A \leftarrow B: r_B$;
2. $A \leftarrow B: k \oplus h_{kAB}(r_B, B)$.

Если требуется двусторонняя аутентификация, то можно модифицировать последний протокол, добавив третье сообщение и предоставив возможность участнику A путем генерации случайного числа r_A и введения его в сообщение на втором шаге протокола, убедиться на третьем шаге в том, что он имеет дело именно с участником B, а также в том, что участник B получил правильное значение ключа k:

1. $A \leftarrow B: r_B$;
2. $A \rightarrow B: E_{kAB}(k, r_A, r_B, B)$,
3. $A \leftarrow B: E_k(r_A)$.

Исходный протокол можно модифицировать так, чтобы искомый ключ k генерировался не одной стороной, а являлся результатом двустороннего обмена. Пусть участники A и B помимо случайных чисел r_A и r_B генерируют случайные числа k_A и k_B соответственно, тогда в результате выполнения протокола:

1. $A \leftarrow B: r_B$;
2. $A \rightarrow B: E_{kAB}(k_A, r_A, r_B, B)$,
3. $A \leftarrow B: E_{kAB}(k_B, r_B, r_A, A)$.

Каждая из сторон может вычислить общий ключ k с помощью некоторой функции / по правилу $k = f(k_A, k_B)$. Подчеркнем, что в этом протоколе ни одна из сторон не может предсказать заранее значения ключа k.

Использование односторонней функции. В этом протоколе участник A имеет право самостоятельно генерировать новый сеансовый ключ k. Получив сообщение на втором шаге, участник B расшифровывает его и проверяет правильность полученного значения $h(r_B)$. Затем он вычисляет проверочное значение $h(r_A)$ и отправляет его участнику A, зашифровав на новом ключе k.

Теперь участник A проверяет правильность значения $h(r_A)$и убеждается в целостности сеанса и подлинности B:

1. $A \leftarrow B: B, r_B;$
2. $A \rightarrow B: A, E_{kAB}(h(r_B), r_A, A, k),$
3. $A \leftarrow B: B, E_k(h(r_A)).$

«Бесключевой» протокол Шамира.Этот протокол иногда называют трехпроходным протоколом Шамира— Ривеста — Адлемана(A. Shamir, R. L. Rivest, L. M. Adleman).

Пусть имеется некоторое коммутирующее шифрующее преобразование E. Это означает, что при всех сообщениях x и произвольных ключахk_1 и k_2выполняется равенство

$E_{k1}(E_{k2}(x))=E_{k2}(E_{k1}(x))$.

Тогда пользователи Aи B могут реализовать следующий трехпроходный протокол для передачи секретного ключаk от A к B:

1. $A \rightarrow B: E_{kA}(k);$
2. $A \leftarrow B: E_{kB}(E_{kA}(k)),$
3. $A \rightarrow B: D_{kA}, E_B((E_{kA}(k)))=E_{kB}(k)$.

Заметим, что в этом протоколе можно использовать не каждое коммутирующее преобразование E. Например, легко видеть, что для преобразования$E_{kA}(k)=k \oplus E$ протокол оказывается заведомо нестойким. Поэтому в протоколе Шамира рекомендуется использовать преобразование вида$E_{kA}(k)=k^a \bmod \rho,$ в котором константа a определяется ключомk_A, ρ — большое простое число.

Вместе с тем в данном протоколе отсутствует аутентификация сторон. Поэтому противник может, заблокировав передачу к участнику B, выступить от имени участника B и получить от A ключ для связи с ним от имени B:

1. $A \leftarrow C(B): E_{kA}(k);$

2. $A \leftarrow C(B): E_{kC}(E_{kA}(k))$,

3. $A \leftarrow C(B): E_{kC}(k)$.

Заметим, что протокол не является стойким и к атаке повторением (replayattack). Например, в результате простой атаки:

1. $A \rightarrow C(B): E_{kA}(k)$;

2. $A \leftarrow C(B): E_{kA}(k)$,

3. $A \rightarrow C(B): k$.

ключ может появиться в канале связи в явном виде. Для ее проведения нарушитель C осуществляет доступ к сети от имени участника B, повторяя первое сообщение участника A.

Если для защиты протокола от этой атаки осуществлять проверку на втором шаге в целях отбраковки повторно переданных сообщений, то можно осуществить аналогичную атаку путем чередования сообщений двух различных сеансов (interleavingattack):

$1.A \rightarrow C(B): E_{kA}(k)$;

$1'.A \rightarrow C(B): E_{kA}(k')$;

$2'.A \leftarrow C(B): E_{kA}(k)$;

$3'.A \rightarrow C(B): k$;

$2.A \leftarrow C(B): M$;

$3.A \rightarrow C(B): D_{kA}(M)$,

Здесь M — произвольное фиктивное сообщение.

2. Анализ криптографических средств защиты информации

В настоящее время производители различных фирм и компаний выпускают огромное количество аппаратных криптографических модулей, простейшие из которых реализованы аналогично смарт-картам, подключаемым к USB-порту компьютера. Выпускаемые криптографические модули, как правило, помимо функций формирования и проверки ЭЦП,

имеют и другие функциональные возможности. Поскольку криптографические преобразования - шифрование и ЭЦП - признаются единственным надежным способом защиты информации, передаваемой по каналам связи, мобильные аппаратные криптографические модули зачастую содержат функции шифрования, ЭЦП, хэширования, генерации ключей, долговременного хранения ключей и сертификатов.

Ниже приводятся описания, основные функциональные возможности и характеристики наиболее распространенных криптографических модулей.

USB-ключи. Первым в Россиик выпуску аппаратных персональных средств защиты информации приступил коллективОсобого конструкторского бюро систем автоматизированного проектирования который, начав с выпуска USB-токена - аналога смарт-карт, перешел к целому семейству ШИПКА на микропроцессорах, покрывающему все современные задачи открытой криптографии. Средства защиты информации в форм-факторе USB-ключ бывают довольно разные, но достаточно легко группируются в три класса: USB-токены, изделия типа HASP и ПСКЗИ.

USB-токены. USB-токен это USB-устройство, построенное на смарт-карточном кристалле. И именно это определяет их функциональную идентичность, поскольку функциональность смарт-карты строго ограничена возможностями ее микросхемы. Этих возможностей вполне достаточно для того, чтобы реализовать различные процедуры аутентификации, в том числе для аутентификации с использованием криптографических алгоритмов, ЭЦП или шифрования. Такие изделия могут применяться для аутентификации при локальном входе в компьютер, входе в домен Windows, для шифрования или подписи сообщений электронной почты, получения сертификатов подписи – для использования инфраструктуры PKI.

В USB-токенеШипка-1.5 аппаратно реализованы все стандартные российские криптографические алгоритмы. Аппаратная реализация вычислений - без привлечения ресурсов компьютера — это важное отличие устройства

Шипка-1.5 от других известных решений на базе USB-ключей, которые фактически представляют собой только энергонезависимую память и адаптер USB-интерфейса, а весь критичный уровень вычислений реализован программно.

Устройство Шипка-1.5 является полностью программируемым. Шипка-1.5 явилось первым в свое время единственным аппаратным ПСКЗИв России.

Изделия типа HASP. HASP - это система защиты программ и данных от нелегального использования и несанкционированного распространения. Механизм ее использования примерно такой - в комплект поставки ПО, помимо собственно ПО на том или ином носителе, входит также USB-ключ, необходимый для того, чтобы подтвердить легальность копии - без этого ключа ПО работать не будет.

Соответственно возможность легального использования этого ПО должна быть связана именно с определенным владельцем, а не с определенным компьютером.

Персональное средство криптографической защиты информации ШИПКА. Архитектура обеспечивает возможность наращивания ресурсов, а также способность быть перепрограммируемым. Оба эти требования выполняются при использовании микропроцессора

Базовым элементом ПСКЗИ ШИПКА является микропроцессор, имеющий собственную энергонезависимую память.

Взаимодействие ПСКЗИ ШИПКА и ПК может быть организовано через различные интерфейсы.

Задачи, которые можно решать с помощью ПСКЗИ ШИПКА разных версий, можно разделить на три большие группы:

- создание защищенной и одновременно мобильной персональной информационной среды и защита информационного взаимодействия граждан и организаций;

- создание корпоративных систем защищенного электронного документооборота разного уровня сложности, внедрения и использования ЭЦП и работа с Удостоверяющими центрами и пространством PKI;

- разработка специализированных приборов и устройств, включающих криптографическую подсистему.

Достоинством ПСКЗИ ШИПКА, важным для решения всех трех групп задач, является ее перепрограммируемость. В основе устройства - универсальный перепрограммируемый микропроцессор, а это значит, что:

– функциональность устройства может быть изменена под те или иные требования, что делает интеграцию устройства в различные системы более удобной;

– набор реализованных в криптографической библиотеке алгоритмов может включать в себя те алгоритмы, которые предпочтительнее для тех или иных задач и не содержать никаких других, а может предоставлять пользователю возможность выбора, если это предусмотрено политикой безопасности.

Семейство ШИПКА. ПСКЗИ ШИПКА представляет собой специализированное мобильное устройство, позволяющее надежно выполнять криптографические преобразования и хранить ключи

Семейство включает в себя серию USB-устройств:

ШИПКА-1.5, ШИПКА-1.6 и ШИПКА-1.7, а также устройства в конструктиве CF Type II, PCCARDTypeII, ExpressCard34 и устройство ШИПКА-Модуль.

Криптографическая функциональность всех этих устройств одинакова - это шифрование, ЭЦП, хэш-функция, генерация ключей, долговременное хранение ключей и сертификатов. Реализация криптографических операций во всех случаях аппаратная (по отношению к ПК).

Все устройства являются полностью перепрограммируемыми и может обновляться непосредственно пользователем. Это дает возможность

расширения его функциональности и создания индивидуальных решений для тех или иных задач заказчика, в случаях, когда эксклюзивное решение предпочтительнее стандартного.

Архитектура ПСКЗИ ШИПКА-1.6 включает аппаратный сопроцессор, что позволяет не тратить ресурсы микропроцессора на криптографические вычисления, но тем не менее осуществлять их в доверенной среде

Логика аппаратного сопроцессора позволяет выполнять криптографические операции аппаратно, но в то же время существенно быстрее, чем микропроцессором устройства, поскольку сопроцессор сконфигурирован специально для выполнения криптографических преобразований, и, стало быть, выполняет их намного эффективнее.

Архитектура ШИПКА-1.6 дает возможность динамически перепрограммировать сопроцессор на нужный набор аппаратных функций. Это значит, что фактически все эти алгоритмы доступны одновременно.

ШИПКА-1.7 - устройство принципиально другого уровня по отношению как к модификации ШИПКА-1.5, так и к ШИПКА-1.6, в первую очередь потому, что работает в режиме USB High-Speed.

Использование USB-контроллера High-Speed обеспечивает производительность устройства до следующих показателей:

- вычисление хэш-функции происходит со скоростью около 3 Mbyte/s;
- шифрование - со скоростью около 1.5 Mbyte/s.

Устройство ШИПКА-Модуль является вариантом изделия Шипка-1.6, имеющим интерфейсы типа I2C (100 Kbit, 400 Kbit) или UART (до 115200 бод).

Конструктивно выполнено в виде модуля 25x25x15 mm, имеющего14 штыревых выводов. Модуль предназначен для монтажа на печатную плату. Имеет повышенную влагостойкость и вибропрочность.

Разборка устройства механически затруднена (модуль залит жестким компаундом), однако даже если ее осуществить - криптографические критичные

данные извлечь будет невозможно из-за архитектурных особенностей примененной элементной базы.

Если от ПСКЗИ требуется повышенная производительность при реализации алгоритмов шифрования, то использование USB-устройства нецелесообразно: даже при реализации в ПСКЗИ интерфейса типа USB 2.0 HighSpeed приемлемого уровня интегрального снижения производительности получить невозможно

ruToken. ruToken - это аппаратное средство аутентификации и защиты информации, использующее алгоритмы шифрования и аутентификации и объединяющее в себе несколько международных стандартов безопасности. Производитель – Российская фирма «АНКАД»

ruToken представляет собой небольшое электронное устройство, подключаемое к USB-порту компьютера (USB-брелок). Он является аналогом смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель).

Поддержка промышленных стандартов позволяет встраивать ruToken в общеупотребительное программное обеспечение, а использование алгоритма шифрования позволяет создавать на базе идентификаторов ruToken системы информационной безопасности.

ruToken может применяться в любых приложениях, где традиционно используются пароли, смарт-карты и другие идентификаторы.

В комплексе с соответствующими программно-аппаратными средствами ruToken может использоваться для решения следующих задач: аутентификация, защита данных и корпоративное использование.

Идентификаторы ruToken. Электронный идентификатор– это компактное устройство в виде USB-брелка, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных.

ruToken заменяет парольные системы защиты, все пароли надежно хранятся в памяти токена. Все, что должен сделать пользователь - подключить токен к USB-порту и набрать PIN-код. Таким образом, осуществляется двухфакторная аутентификация, когда доступ к информации можно получить, только обладая уникальным предметом (токеном) и зная некоторую уникальную комбинацию символов (PIN-код)

ruToken - это аналог смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель), данные надежно хранятся в энергонезависимой памяти токена объемом до 128 Kbyte, прочный корпус ruToken устойчив к внешним воздействиям.

Основу ruToken составляет микроконтроллер, который выполняет криптографическое преобразование данных, и память, в которой хранятся данные пользователя (пароли, сертификаты, ключи шифрования и т. д.).

Главным отличием ruToken от зарубежных аналогов является аппаратно реализованный российский стандарт шифрования - ГОСТ 28147.

Электронные ключи iKey. Электронные ключи iKey от компании RainbowTechnologies предназначены для защиты цифровой идентичности в рамках PKI. В изделии с помощью аппаратных средств генерируются и хранятся пары открытых ключей и цифровые сертификаты, а также производится электронная цифровая подпись.

iKey обеспечивает создание системы защиты и криптографического кодирования непосредственно внутри устройства, предлагая тем самым оптимальное решение проблемы безопасной аутентификации пользователя. Подключается к любому стандартному USB-порту, действуя одновременно как смарткарта и считыватель, заключенные в едином устройстве с конструктивном USB.

iKey рекомендуется использовать для решения следующих задач:

- идентификация и строгая двухфакторная аутентификация пользователя;

- аутентификация пользователя при доступе к защищенным корпоративным данным через SSL;

- аутентификация пользователя при доступе к защищеннымWeb-ресурсам;

- хранение цифровых сертификатов и закрытых ключей пользователя;

- обеспечение безопасного входа в сеть предприятия с любой рабочей станции;

- автоматическая блокировка рабочей станции при извлечении iKey;

- поддержка аутентификации в VPN-клиентах;

- защита электронной почты.

Применение iKey повышает уровень защищенности информации на компьютере без дополнительных затрат на приобретение и установку специального программного обеспечения.

Комплект iKey включает аппаратные электронные ключи, выполненные в двух форм-факторах (USB-ключ и смарт-карта), набор драйверов и прикладных программ для обеспечения доступа к защищаемым объектам.

USB-ключи MS_Key. Разработчиком и производителем ключа MS_Key является компания «Мультисофт». Этот ключ на текущий момент является уникальным решением, в котором используется сертифицированный аппаратный модуль, реализующий российские криптографические алгоритмы.

Криптографическая реализация имеет сертификат Федеральной службы безопасности Российской Федерации на соответствие ГОСТ 28147, ГОСТ Р 34.10 и требованиям к СКЗИ и может использоваться для реализации функций формирования и проверки электронной цифровой подписи и шифрования информации, не содержащей государственную тайну.

Главное достоинство этого USB-ключа – формирование ЭЦП клиента непосредственно внутри него.

Целевыми сферами применения являются:

- удаленный банковский клиент (система клиент-банк). С помощью ключа MS_Key клиент подписывает ЭЦП платежные поручения на аппаратном уровне;

- защищенный документооборот. MS_Key используется для аутентификации пользователей системы;

- системы сбора налоговой отчетности (предоставление налоговой отчетности в электронном виде) Ключи могут использоваться в системе Федеральной Налоговой Службыи на клиентской стороне (организация, сдающая отчет).

- системы сбора статистической отчетности (предоставление статистической отчетности в электронном виде). Ключи могут использоваться в системе Государственного комитета статистики России и на клиентской стороне (организация, сдающая статистический отчет).

- органы власти и управления. Использование ЭЦП в органах государственной власти

- и многие другие.

eToken. eToken — это первый полнофункциональный аналог смарт-карты, выполненный в виде брелка. Он напрямую подключается к компьютеру через USB-порт и не требует наличия дорогостоящих считывателей смарт-карт или других дополнительных устройств.

eToken имеет до 64 Kbyte защищённой энергонезависимой памяти (EEPROM) и может использоваться как портативный контейнер для хранения секретных данных (ключей шифрования, паролей, сертификатов и пр.).

eToken имеет УНИКАЛЬНЫЙ СЕРИЙНЫЙ НОМЕР(ID) и может использоваться как электронный идентификатор (ключ) для аутентификации пользователя. eToken поддерживает работу и интегрируется со всеми основными системами и приложениями, использующими технологию PKI.

eToken выпускается в виде двух форм-факторов: как в виде USB-КЛЮЧА, так и в виде СМАРТ-КАРТ.

Назначение:

- аутентификация пользователей при доступе к защищённым ресурсам, серверам, защищённым страницам Web-сайтов;
- защита электронной почты (ЭЦП, шифрование);
- обеспечение безопасности финансовых транзакций, систем «Клиент-банк», «Домашний банк»;
- защита сетей и компьютеров, аутентификация при работе с VPN;
- хранение секретной информации: паролей, ключей шифрования, цифровых сертификатов.

eToken может использоваться в любых приложениях для замены паролей на более надёжную аппаратно-программную аутентификацию. В прикладных программах применяется для хранения служебной информации разработчиков, персональной информации пользователей, паролей, криптографических ключей и пр.

Преимущества:

- Строгая аутентификация. eToken позволяет осуществлять одно- или двухфакторную аутентификацию. Это намного надёжнее, чем использование паролей.
- Высокая защищенность. Секретная информация хранится в защищенной памяти ключа.
- Доступ к памяти защищен PIN-кодом. Если eToken был потерян или украден, то злоумышленник воспользоваться им не сможет.
- Компактность и удобство. Электронные ключи eToken имеют небольшой размер, легко размещаются на связке с ключами. Выпускаются в герметичных цветных корпусах и имеют световую индикацию режимов работы.

- Быстрое встраивание. eToken поддерживает большинство современных стандартов и API, легко встраивается как в существующие приложения, так и в новые. Поддержка смарт-карт (PC/SC) стандарта позволит без труда перейти от смарт-карт к ключу eToken.

- Уникальность. Каждый eToken имеет 32-битный ID, доступный только для чтения.

- Нужен всего один брелок**.**eToken одновременно может использоваться различными приложениями, поэтому пользователю нет необходимости носить с собой целую связку ключей eToken.

- Возможна одновременная работа с несколькими ключами eToken.

- Персонализация ключей eToken позволяет каждому ключу присвоить уникальное имя его владельца.

- Простота использования. ПерсонализированныйeToken достаточно подключить к порту USB и, при необходимости, ввести PIN-код. Порт USB имеется во всех современных компьютерах, ноутбуках, во многих моделях мониторов и клавиатур.

LUNA SA HSM. LUNA SA HSM является высокопроизводительным аппаратным модулем безопасности общего назначения для построения PKI, ускорения IPsec/SSL - операций и других криптоопераций.

Отличается высочайшей производительностью – до 5 500 операций RSA-1024 Sign в секунду.

Благодаря большому количеству поддерживаемых алгоритмов, программных интерфейсов и платформ, Luna SA может использоваться для выполнения практически любых криптографических задач, однако устройство было специально оптимизировано для:

- эффективной работы с асимметричными алгоритмами (как традиционными, так и на эллиптических кривых);

- безопасного хранения ключей;

- работы в корпоративной среде (функции высокой доступности и двухуровневой авторизации).

Чип безопасности TRM. Предложенный некоммерческой международной организацией TrustedComputingGroup (TCG) доверенный модуль TrustedPlatformModule (TPM) представляет собой микроконтроллер, выполненный в виде интегральной микросхемы, которую принято называть чипом безопасности. Микроконтроллер хранит ключи, пароли и цифровые сертификаты. Обычно он встроен в системную плату компьютера, а потенциально может быть использован в любом устройстве, так как его размер не превышает размера мелкой монеты.

Реализация чипа гарантирует, что хранимая в нем информация надежно защищена как от физического взлома, так и от атак со стороны внешнего программного кода. Защитные механизмы платформ способствуют разработке и применению сервисов безопасности. Технологии безопасности, основанные на открытом ключе (PKI), такие как ЭЦП и протоколы обмена ключами, защищаются посредством подсистем, реализованных по стандарту TCG. Доступ к данным и секретам платформы может быть запрещен, если параметры процесса загрузки ОС отклонятся от заданных значений. В силу этого критичные приложения и процессы, обеспечивающие защиту веб-доступа, электронной почты и локальных данных, при установке на доверенную платформу TCG становятся все более и более неуязвимыми.

В чип установлены алгоритмы асимметричной криптографии, обеспечивающие высокий уровень защиты.

Стойкость криптографических средств является определяющим основным признаком при выборе того и/или другого средства криптографической защиты. Она определяется, в первую очередь, стойкостью используемых алгоритмов ЭЦП, шифрования и хэширования. Однако, подавляющее большинство криптографических модулей

зарубежного производства, например LUNASAHSM, чип безопасности TRM и семейство ШИПКА,применительно к алгоритмуRSA,используют нестойкие функции хэшированияMDx, SHA-1, SHA-2, которые уязвимы к универсальным атакам

. С этой точки зрения, в основном, криптографические модули, реализующие алгоритмы по Российским национальным стандартам на сегодня обеспечивают самый высокий уровень стойкости.

Способ подключения криптографического модуля к компьютеру или другим устройствам, элементная база и памятьнаходятся в зависимости от функциональных возможностей и чем проще сконструирован модуль, тем проще способ его подключения.Простейшие аппаратные криптографические модули подключаются к USB-порту компьютера, модули со сложной архитектурой встраиваются в ПК.

3.Национальные криптографические средства защиты информации

Устройство SIT-1. Аппаратно-программное USB – устройство SIT-1 является первым опытным вариантом криптографического модуля ЭЦП, разработанным в ГУП «UNICON.UZ» УзАСИ в 2008 г. Основу устройства составляет микроконтроллер. Предназначен для реализации O‘z DSt 1092.

В ходе реализации устройства SIT-1 практически отработаны следующие вопросы:

- разработан алгоритм работы устройства в соответствии с O‘z DSt 1092;
- разработано программное обеспечение для микроконтроллеров, составляющих основу устройства, а также драйвер устройства для ОС WindowsXP;
- приведено краткое описание библиотеки функций программного интерфейса, предназначенного для взаимодействия пользовательских программ с устройством;

- изготовлен макетный образец устройства и проведены его тестовые испытания.

Проанализировав технические данные предлагаемых СКЗИ на мировом рынке, можно сделать вывод, что существует несколько критериев, по которым можно классифицировать практически все существующие СКЗИ:

- по способу реализации;
- по функциональному предназначению;
- по стойкости алгоритмов шифрования и криптографических протоколов;
- по методу шифрования;
- по принципу работы шифраторов;
- по функциональному расположению в криптосистеме.

В связи с тенденцией развития в последнее время многофункциональных СКЗИ, объединяющих в себе несколько уровней и методов криптографической защиты, приведенная классификация носит условный характер.

Система защищенной электронной почты «E-XAT»

Система защищенной электронной почты E-XAT предназначена для организации защищенного обмена электронными сообщениями между корпоративными клиентами – пользователями системы E-XAT. Защищенность обмена сообщениями обеспечивается за счет использования криптографических преобразований:

– шифрования данных - каждое отправляемое почтовое сообщение шифруется;

– электронной цифровой подписи – каждое отправляемое электронное сообщение подписывается электронной цифровой подписью отправителя.

Система E-XAT обеспечивает:

– *Идентификация* – доступ к системе осуществляется только при наличии секретного ключа, а также набором соответствующих пользователю идентификационных данных (логин и пароль). После успешной идентификации пользователь получает доступ к системе E-XAT.

– *Конфиденциальность* – все электронные почтовые сообщения шифруются отправителем при их отправке. Электронные почтовые сообщения остаются в зашифрованном виде при их передаче по сети и при хранении на почтовом сервере. Расшифровать электронное почтовое сообщение может только адресат при открытии почтового сообщения, а также сам отправитель. Благодаря этому, почтовые сообщения могут передаваться по незащищенным каналам передачи данных, в том числе Интернет.

– *Аутентификация* – почтовые сообщения подписываются электронной цифровой подписью отправителя, что позволяет однозначно определить автора почтового сообщения путем проверки его электронной цифровой подписи. Проверка электронной цифровой подписи осуществляется автоматически при открытии почтового сообщения.

– *Целостность электронных сообщений* – проверка неискаженности (неизменности) информации в электронном сообщении с момента его подписания до получения его получателем обеспечивается с помощью проверки электронной цифровой подписи. В случае любого (преднамеренного или не преднамеренного) искажения информации подпись в электронных сообщениях считается недействительной.

Устройство защищённого хранения ключа ЭЦП «E-Kalit». Аппаратно-программное устройство E-KALIT является отечественным продуктом, специально разработанным для использования совместно синформационными системами, где требуется защищенное хранение секретных ключей шифрования и ЭЦП: «Банк-клиент», «Интернет банкинг» и других. В настоящее время устройство

интегрировано в такие программные продукты, как E-HUJJAT, E-XAT, HIMFAYL и «Центр регистрации ключей ЭЦП».

E-KALIT представляет собой носимый USB-брелок с небольшими габаритами, обеспечивает хранение личных криптографических параметров пользователя в защищенной доверенной среде, тем самым заменяет такие импортируемые зарубежные средства, как i-Key, eToken и другие.

E-KALIT не имеет файловую систему и при подключении к персональному компьютеру не определяется операционной системой как устройство хранения (флэш-память), благодаря чему стандартный доступ к устройству из других программ невозможен.

Система S-files. Система S-files предназначена для обеспечения безопасности, целостности и защищенности от несанкционированного доступа папок и файлов, хранящихся на персональном компьютере или внешних дисковых носителях информации.

– Применение системы позволяет защитить хранящиеся электронные данные от несанкционированного доступа, просмотра или изменения (искажения).

– Безопасность файлов обеспечивается с помощью использования средств криптографического шифрования данных.

– Целостность данных обеспечивается посредством использования электронной цифровой подписи (ЭЦП) и средств восстановления утерянных данных.

В настоящее время разработанная система не имеет аналогов в республике.

Система «s-files» позволяет

– обеспечить высокий уровень информационной безопасности корпоративной сети;

– обеспечить безопасность и целостность файлов пользователей;

– предотвратить случаи несанкционированного доступа к информации;

– сократить финансовые потери от нарушения целостности и утери информации;

– повысить защищенность служебной информации и информации с ограниченным доступом.

Таблица 2.

Результаты сравнительного анализа существующих аппаратных криптографических моделей

Признаки	**LUNA SA HSM**	**Чип безопасности TRM**	**USB-токен (семейства ШИПКА)**	**Устройство «E-Kalit»**
Стойкость	Низко-средняя	Низкая	Низко-средне-максималь-ная	Низко-средне-максимальная
Производительность	Высокий	Средний	Низкий	Высокий
Функциональные возможности	Асимметричные криптоалгоритмы, хранение секретных ключей и цифровых сертификатов	Асимметричные криптоалгоритмы, хранение секретных ключей и цифровых сертификатов	Шифрование, ЭЦП, хэш-функция, генерация и хранение ключей и сертификатов	Асимметричные криптоалгоритмы, хранение защищенное хранение секретных ключей шифрования и ЭЦП

4. Анализ свойств межсетевых экранов, используемых в корпоративных сетях

Пакетный уровень.

Межсетевые экраны с пакетной фильтрацией.

Межсетевые экраны с пакетной фильтрацией могут также быть программными пакетами, базирующимися на операционных системах общего назначения (таких как Windows и Unix) либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Аналогично межсетевым экранам прикладного уровня, доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.

Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния). Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена передача только определенных пакетов. Рассмотрим в качестве примера последовательность установки соединения. Первый ожидаемый пакет - пакет SYN. Межсетевой экран обнаруживает этот пакет и переводит соединение в состояние SYN. В данном состоянии ожидается один из двух пакетов - либо SYNACK (опознавание пакета и разрешение соединения) или пакет RST (сброс соединения по причине отказа в соединении получателем). Если в данном соединении появятся другие пакеты, межсетевой экран аннулирует или отклонит их, так как они не подходят для данного состояния соединения, даже если соединение разрешено набором правил.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране (рис 3), а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и состояние соединения правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое - для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

Рис. 4. Передача трафика через межсетевой экран с фильтрацией пакетов

Как правило, межсетевые экраны с фильтрацией пакетов имеют возможность поддержки большего объема трафика, т. к. в них отсутствует

нагрузка, создаваемая дополнительными процедурами настройки и вычисления, имеющими место в программных модулях доступа.

Последний абзац начинается с фразы «как правило». Различные производители межсетевых экранов сопоставляют их производительность различными способами. Исторически сложилось так, что межсетевые экраны с пакетной фильтрацией имеют возможность обработки большего объема трафика, нежели межсетевые экраны прикладного уровня, на платформе одного и того же типа. Это сравнение показывает различные результаты в зависимости от типа трафика и числа соединений, имеющих место в процессе тестирования.

Преимущества пакетного уровня:

- низкая стоимость;
- высокая производительность.

Недостатки:

- сложность конфигурирования и поддержки;
- отсутствие дополнительных возможностей;
- рухнувшая сеть остается открытой (не защищенной);
- не защищены от фальсификации IP- и DNS-адреса.

Прикладной уровень.

Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня, или прокси-экраны, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения (таких как Windows и Unix) или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

Правила политики безопасности усиливаются посредством использования модулей доступа. В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа. Лучшими модулями доступа считаются те, которые построены специально для разрешаемого протокола. Например, модуль доступа FTP предназначен для протокола FTP и может определять, соответствует ли проходящий трафик этому протоколу и разрешен ли этот трафик правилами политики безопасности.

При использовании межсетевого экрана прикладного уровня все соединения проходят через него. Как показано на рис 2, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений. Здесь подразумевается, что модуль доступа на межсетевом экране сам по себе неуязвим для атаки. Если же программное обеспечение разработано недостаточно тщательно, это может быть и ложным утверждением.

Дополнительным преимуществом архитектуры данного типа является то, что при ее использовании очень сложно, если не невозможно, «скрыть» трафик внутри других служб. Например, некоторые программы контроля над системой, такие как NetBus и BackOrifice, могут быть настроены на использование любого предпочитаемого пользователем порта.

Следовательно, их можно настроить на использование порта 80 (HTTP). При использовании правильно настроенного межсетевого экрана прикладного уровня модуль доступа не сможет распознавать команды, поступающие через соединение, и соединение, скорее всего, не будет установлено.

Межсетевые экраны прикладного уровня содержат модули доступа для наиболее часто используемых протоколов, таких как HTTP, SMTP, FTP и telnet. Некоторые модули доступа могут отсутствовать. Если модуль доступа отсутствует, то конкретный протокол не может использоваться для соединения через межсетевой экран.

Межсетевой экран также скрывает адреса систем, расположенных по другую сторону от него. Так как все соединения инициируются и завершаются на интерфейсах межсетевого экрана, внутренние системы сети не видны напрямую извне, что позволяет скрыть схему внутренней адресации сети.

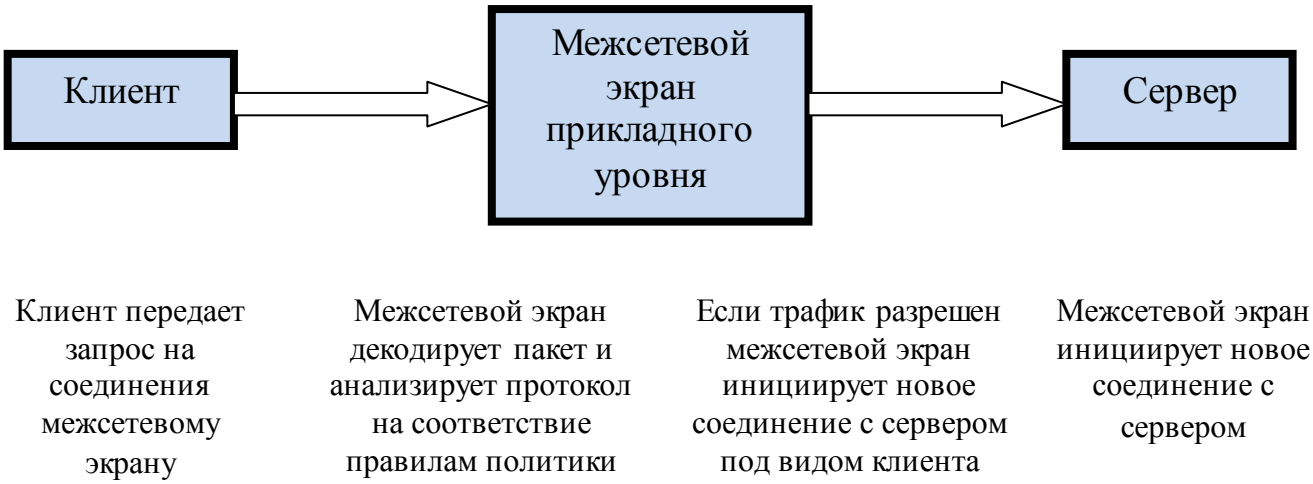

Рис3. Соединения модуля доступа межсетевого экрана прикладного уровня

Большая часть протоколов прикладного уровня обеспечивает механизмы маршрутизации к конкретным системам для трафика, направленного через определенные порты. Например, если весь трафик,

поступающий через порт 80, должен направляться на веб-сервер, это достигается соответствующей настройкой межсетевого экрана.

Преимущества прикладного уровня:

- маскировка защищаемой сети;
- широкие возможности (усиленная аутентификация, детальное протоколирование);
- рухнувшая сеть остается заблокированной (защищенной).

Недостатки:

- высокая стоимость;
- низкая производительность.

Идеальный персональный межсетевой экран должен выполнять шесть функций:

Блокировка внешних атак. В идеале межсетевой экран должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр.

Блокировка утечки информации.Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), межсетевой экран должен предотвратить утечку информации, заблокировав вирусу выход в сеть.

Контроль приложений. Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Кроме банальной проверки по имени файла, весьма желательна проверка аутентичности приложения.

Поддержка зональной защиты. Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как

правило, потенциально опасных) технологий. В то же время уровень доверия к Интернет-контенту значительно ниже, а значит, необходим дифференцируемый подход к анализу опасности того или иного содержания.

Протоколирование и предупреждение. Межсетевой экран должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются.

Максимально прозрачная работа. Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении «мастеров» (Wizards) по настройке и прочих инструментов, даже опытные администраторы не пренебрегают ими просто в целях экономии времени[21].

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.

Принципы работы межсетевых экранов. Существует два основных способа создания наборов правил межсетевого экрана: «включающий» и «исключающий». Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам и блокирует все остальное.

Включающий межсетевой экран обеспечивает гораздо большую степень контроля исходящего трафика. Поэтому включающий межсетевой экран является лучшим выбором для систем, предоставляющих сервисы в

сети Интернет. Он также контролирует тип трафика, порождаемого вне и направляющегося в вашу приватную сеть. Трафик, не попавший в правила, блокируется, а в файл протокола вносятся соответствующие записи. Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

Безопасность может быть дополнительно повышена с использованием «'межсетевого экрана с сохранением состояния»'. Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (DenialofService, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что позволяет создавать оптимальную конфигурацию для каждой конкретной системы.

На рис.5 показано блокирование proxy-сервером прямого IP-трафика между локальной сетью и Интернет. Пользователь пытается загрузить Web-страницу из Интернет. Поскольку его браузер настроен так, чтобы отправлять все HTTP-запросы через proxy-сервер, они никогда не будут посылаться Web-серверу напрямую.

Запрос поступит к proxy-серверу по подключенному к локальной сети адаптеру. Proxy-сервер не осуществляет маршрутизацию (или пересылку) IP-пакета с запросом заданному серверу в Интернет. Вместо этого proxy-сервер, руководствуясь заданными администратором правилами, проверяет, разрешен ли запрос. Если да, то proxy-сервер формулирует запрос страницы от своего имени, используя в качестве адреса отправителя адрес своего внешнего сетевого адаптера (подключенного к Интернет). Принявший этот

запрос Web-сервер в Интернет считает proxy-сервер клиентом, запросившим страницу, и возвращает данные ему.

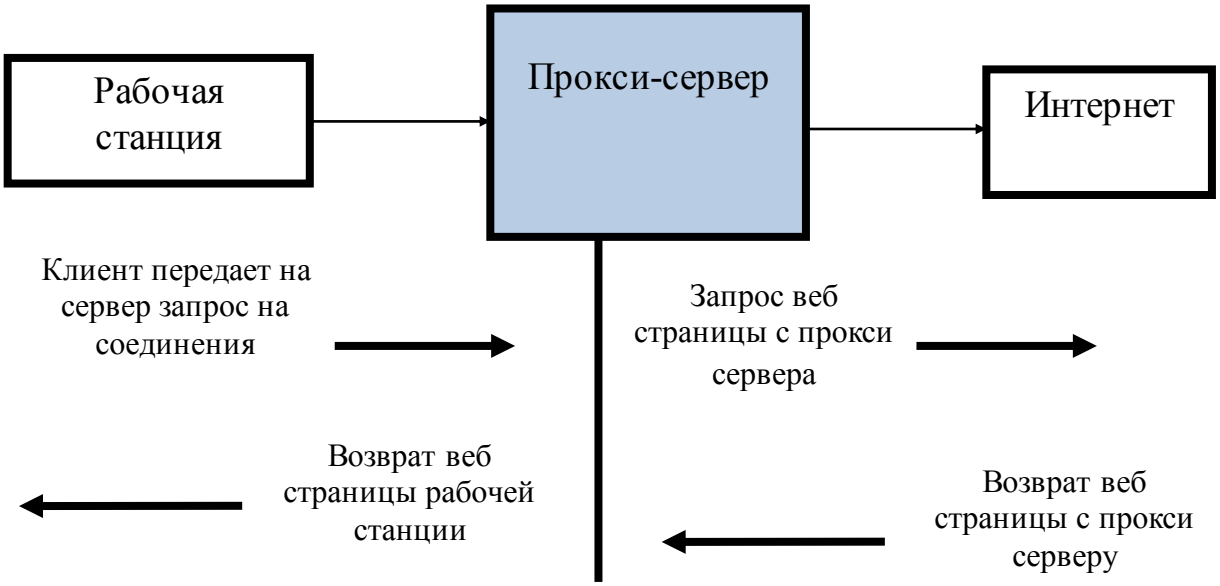

Рис. 5. Прокси-сервер образует рубеж, через который не проникают IP-пакеты

Здесь IP-пакеты блокируются за счет выключения маршрутизации в двухканальном proxy-сервере.

После получения запрошенной Web-страницы proxy-сервер не передает IP-пакеты клиенту, а производит ряд заданных администратором проверок пришедших данных. Если все в порядке, proxy-сервер создает новые IP-пакеты с адресом своего адаптера локальной сети и возвращает Web-страницу клиенту.

Таким образом, блокирование IP-трафика - не единственное преимущество proxy-сервера. С его помощью выполняются определенные проверки на основе набора заданных вами правил, в результате чего proxy-сервер будет пропускать или отбрасывать поступившие данные.

Каждая из работающих через межсетевой экран сетевых служб нуждается в отдельной программе proxy-сервера. Для стандартных служб TCP/IP, таких как Telnet, FTP или HTTP, существует множество proxy-

серверов. Но не исключено, что вам не удастся найти proxy-сервер для каких-либо новых или редко используемых служб. Имеются настраиваемые proxy-серверы, но они обеспечивают меньшую степень защиты, чем proxy-серверы, привязанные к приложению.

*Работа с Proxy.*Чаще всего для работы с различными типами Proxy используют программы, которые помогают быстро и легко (а иногда и наоборот) настроится на определенные Proxy сервера (прокси), а также проверить их на работоспособность и создать «цепочку анонимности» из них.

Принцип работы практически всех программ, работающих с Proxy серверами выглядит как показано на рисунке 6.

Выше представленная схема показывает доступ к различным сервисам интернета через один Proxy сервер.

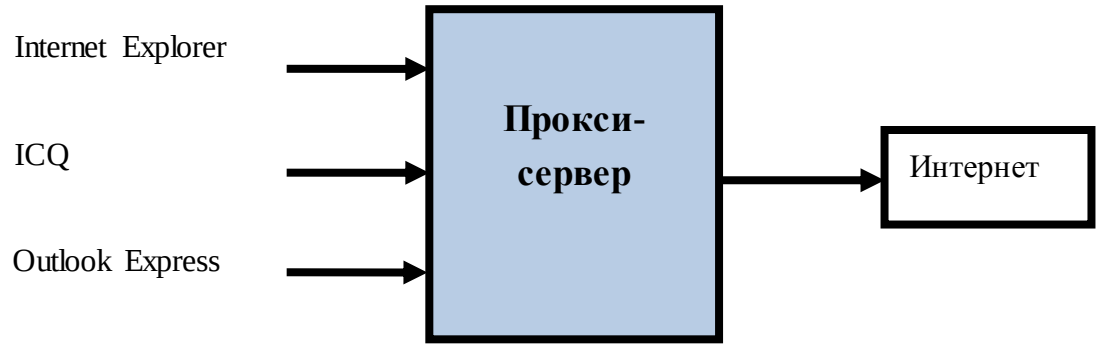

Рис. 6. Принцип работы с прокси-серверами

Аналогично этому, можно составить цепочку Proxy серверов, для большей анонимности (рис. 7).

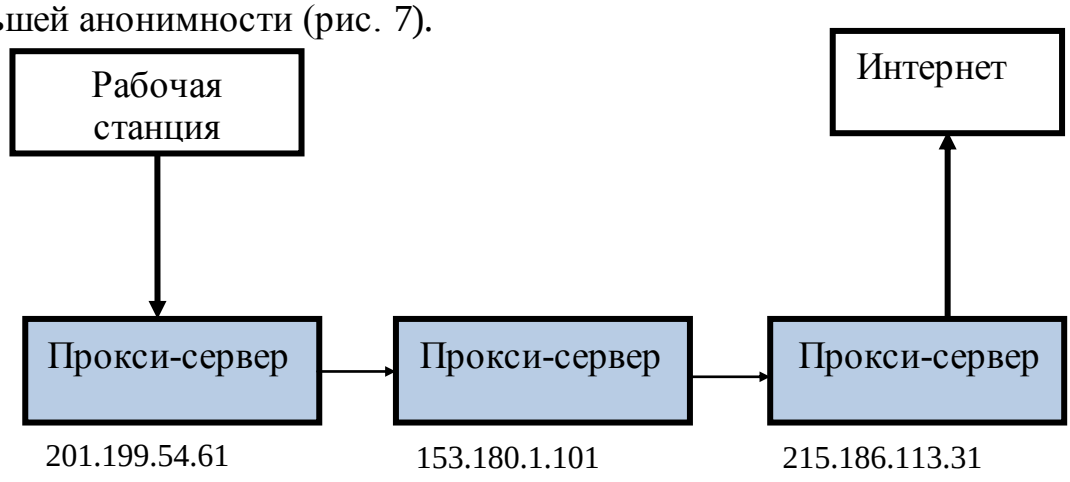

Рис. 7. Цепочка прокси-серверов

В данной схеме доступа в Интернет, представлена цепочка в виде 3 последовательных Proxy серверов, которые последовательно друг другу передают определенный, заданный запрос (например от InternetExplorer на просмотр страницы с сайта www.mail.ru).

Проще выражаясь: компьютер пользователя подает запрос на открытие Web-сайта первому Proxy серверу, тот в свою очередь передает этот запрос второму Proxy серверу, но уже от своего имени (т.е. заменяя «реальный» IP пользователя на свой «подставной» IP адрес Proxy сервера.

Практическое большинство программ работающих с Интернет имеют возможность подключения к «сети» через Proxy. Однако все же остаются программы которые принудительно необходимо подключать к Proxy серверам, через специально разработанное для этого программное обеспечение. Обычно этим ПО, являются мелкие программы, до 1 Мб, но с незаменимыми возможностями. Узнать о возможности подключения той или иной программы через Proxy можно в самой программе, внимательно и полностью изучив ее настройки.

Следует помнить, что многие, а практически и даже все бесплатные Proxy сервера хоть и скрывают настоящий IP адрес пользователя, зато сами ведут статистику и полный учет запросов проходящих через них, т.е. на таких Proxy серверах остаются «логи» (*.log файлы), свидетельствующие о пребывании на расположенных в разных точках мира, также не поможет остаться пользователю полностью анонимным в сети Интернет.

Поскольку proxy-сервер находится между клиентом и сервером, для него подходят следующие методы фильтрации и блокировки контента:

- блокирование URL. Можно блокировать (или регистрировать) доступ к определенным URL. Недостаток этого метода состоит в том, что адреса страниц в Интернет часто меняются. Ежедневно

добавляются тысячи дополнительных страниц, и занятый администратор не всегда в состоянии оценивать все новые сайты;

- блокирование категорий. Метод позволяет задавать категорию блокируемого контента, например сайты с эротическим содержанием или пропагандой ненависти;
- проверка вложений. Некоторые proxy-серверы могут быть настроены для блокирования приложений Java, элементов управления ActiveX и других объектов, которые служат для запуска приложений на локальном компьютере, а значит, всегда имеется риск, что они будут эксплуатироваться хакерами для получения доступа к компьютеру.

Общие компоненты межсетевых экранов

Конфигурация межсетевого экрана — предмет достаточно сложный, и обычно все сетевые экраны (firewall) имеют индивидуальную конфигурацию, отражающую специфику работы конкретной информационной системы. Однако здесь следует придерживаться некоторых общих принципов:

Следует пропускать сквозь себя только те сервисы, которые необходимы для обеспечения требуемой функциональности информационной системы.

Все, что явным образом не разрешено, должно быть запрещено. Это означает, что все службы, не упомянутые при конфигурации межсетевого экрана, должны быть запрещены.

При конфигурации сетевых экранов (firewall) следует вести подробную документацию.

Proxy-сервер (Прокси-сервер). Proxy-сервер регулирует доступ сотрудников компании к ресурсам Интернета. Он имеет гибкие настройки, позволяющие ограничить доступ пользователей к определенным сайтам, контролировать объем выкачиваемой пользователем из Интернета

информации и настраивать возможность доступа в Интернет тех или иных пользователей в зависимости от дня недели и времени суток. Кроме того, proxy-сервер позволяет пользователю не выходить в Интернет со своего адреса, а заменяет при запросах адрес пользователя на свой собственный и посылает запрос уже не от имени реального пользователя сети, а от своего собственного. Это не только помогает скрыть в целях безопасности внутреннюю структуру своей сети, но и позволяет не арендовать дополнительное количество адресов для всех своих сотрудников, а обойтись одним общим адресом для прокси-сервера.

IDS(Система Выявления Атак). IntrusionDetectionSystem (система выявления попыток проникновения) — комплекс программного обеспечения, который обычно устанавливается на межсетевой экран и предназначен для анализа различных событий, происходящих как на самом компьютере с IDS (Host-based IDS), так и в сети вокруг него (Network IDS). Принцип работы host-based IDS основан на анализе журналов событий системы. В основе работы Network IDS лежит анализ сетевого трафика, проходящего через систему. При выявлении события, квалифицируемого IDS как попытка проникновения, ответственному за безопасность системы посылается сообщение об атаке. Одновременно производится запись в журнале атак. Подобное поведение характерно для пассивных IDS. Если же при определенных типах атак система способна производить ряд действий, направленных на отражение атаки, то она относится к активным IDS .

Система контроля целостности ПО и конфигурации. Для более жесткого контроля за попытками проникновения в систему используется многоуровневая защита. Одним из таких дополнительных уровней является система контроля целостности программного обеспечения. Она контролирует все программное обеспечение на брандмауэре и присылает отчеты обо всех удаленных, вновь появившихся и изменившихся файлах. Таким образом, при

малейшем изменении конфигурации шлюза ответственный за его работу получит подробный отчет о том, что и когда было изменено.

Система мониторинга и оповещения о неисправностях. Для максимально быстрого обнаружения неисправностей в компьютерных системах часто применяются системы раннего оповещения о возникающих неисправностях, которые периодически контролируют работоспособность различных сервисов и при любых отклонениях автоматически связываются с обслуживающим систему инженером.

Система удаленного администрирования. Системы удаленного администрирования серверов применяются для устранения неисправностей, конфигурирования систем и выполнения различных рутинных задач в локальной сети (или сети Интернет) без необходимости физического доступа к серверу.

Выводы по второй главе

1. Рассмотрение протоколов распределения ключей показали, что имеются протоколы, в которых стороны осуществляют передачу ключей или обмен ключами при непосредственном взаимодействии, т.е. двусторонние протоколы или, иначе, протоколы типа «точка-точка» и протоколы с централизованным распределением ключей, в которых предусмотрена третья сторона, выполняющая функции доверенного центра.

2. Анализ криптографических средств показали что вподключении криптографического модуля к компьютеру или другим устройствам, элементная база и память находятся в зависимости от функциональных возможностей и чем проще сконструирован модуль, тем проще способ его подключения.

3. Для ограничения доступа хостов внутри сетиприменяются межсетевые экраны, работающие только посредством фильтрации пакетов, не используют модули доступа, и поэтому трафик передается от клиента

непосредственно на сервер. Если сервер будет атакован через открытую службу, разрешенную правилами политики межсетевого экрана, межсетевой экран никак не отреагирует на атаку. Межсетевые экраны с пакетной фильтрацией также позволяют видеть извне внутреннюю структуру адресации. Внутренние адреса скрывать не требуется, так как соединения не прерываются на межсетевом экране.

Глава III. Разработка средств ограничения доступа хостов внутри сети

1. Программный модуль межсетевого экрана.

Для разработки программы в данной работе был выбран язык программирования C#.NET, в виду его гибкости и возможностям расширения.

Перед тем, как начать писать программный код, необходимо понять, как хранится информация в пакетах.

Дейтаграмма- IP инкапсулирует пакеты TCP и UDP. Они содержат данные прикладного уровня модели OSI, такие, как информация от DNS, HTTP, FTP, SMTP, SIP и т.д. Таким образом, пакет TCP получен в дейтаграмме-IP в виде:

IP заголовок	TCP заголовок	Данные

В первую очередь нужно «разбить» пакет на составные части, для дальнейшей фильтрации на основе этих частей.

Средствами C#.NET пакеты можно разбить на части таким образом (пример разбиения IP-заголовка. Для других протоколов разбиение может выглядеть иначе):

```
privatebytebyVersionAndHeaderLength;      // Восемь бит для версии и длины
                                          // заголовка
privatebytebyDifferentiatedServices;      // Восемьбитовдля
                                          // дифференцированных служб
privateushortusTotalLength;               // Шестнадцать бит для общей длины
privateushortusIdentification;            // Шестнадцать бит для идентификации
privateushortusFlagsAndOffset;            // Восемь бит для флагов и смещения
                                          // фрагментации
privatebytebyTTL;                         // Восемьбитдля TTL (Time To Live)
privatebytebyProtocol;                    // Восемь бит для основного
```

```
                                        // протокола
privateshortsChecksum;              // Шестнадцать бит для контрольной
                                    // суммы заголовка
privateuintuiSourceIPAddress;       // Тридцать два бита для IP-адреса
                                    // источника
privateuintuiDestinationIPAddress;  // Тридцать два бита для IP-адреса
                                    // назначения
                                    //Конец заголовка IP
privatebytebyHeaderLength;          //Длина заголовка
privatebyte[]byIPData = newbyte[4096]; //Данные несущие датаграммой
```

Таким образом, уже можно фильтровать проходящие через межсетевой экран пакеты, по IP-адресам и портам источника и назначения, по содержимому заголовков определенных протоколов и по другим критериям.

Разобравшись с правилами фильтрации необходимо определить, как и где будет храниться база с правилами.

В разработанной для данной работы программе база правил хранится в файлах HostConfig.txt (фильтрация по хост-назначения), IpConfig.txt (фильтрация по IP-адрес-назначения), RawConfig.txt(фильтрация по содержимому запроса пользователя) и proxyConfig.txt (общие настройки программы). При запуске программы правила загружаются из вышеописанных файлов и применяются к фильтрации. При добавлении нового правила, оно записывается в соответствующий файл.

На третьем этапе разработки необходимо решить, каким будет интерфейс программы, каким образом пользователи смогут пользоваться данным сервером, и в каком виде будет выдаваться служебная информация администратору и пользователям системы.

Если разработка интерфейса программы не является особой проблемой, так как администратор может сам разобраться в работе программы, то работа

с пользователем должна быть продумана особо хорошо. При невозможности доступа к определенным ресурсам, необходимо выдавать пользователю подробную информацию. При попытке доступа к запрещенным ресурсам также необходимо информировать пользователя. И так со всеми вариантами работы системы, для избегания проблем и недопонимания со стороны пользователей.

После решения всех этих составных частей, можно приступать разработке. И только после многократного тестирования допустимо использование программы в корпоративных сетях, для широкого пользования.

2. Практическое применение межсетевого экрана

При написании данной работы был разработан программный продукт, пользуясь которым можно на практике видеть работу межсетевого экрана с пакетной фильтрацией. Ниже будет приведена инструкция по работе с программой. Программный продукт состоит из исполняемого файла и конфигурационных файлов: HostConfig.txt, IpConfig.txt, keyConfig.txt, proxyConfig.txt и RawConfig.txt.

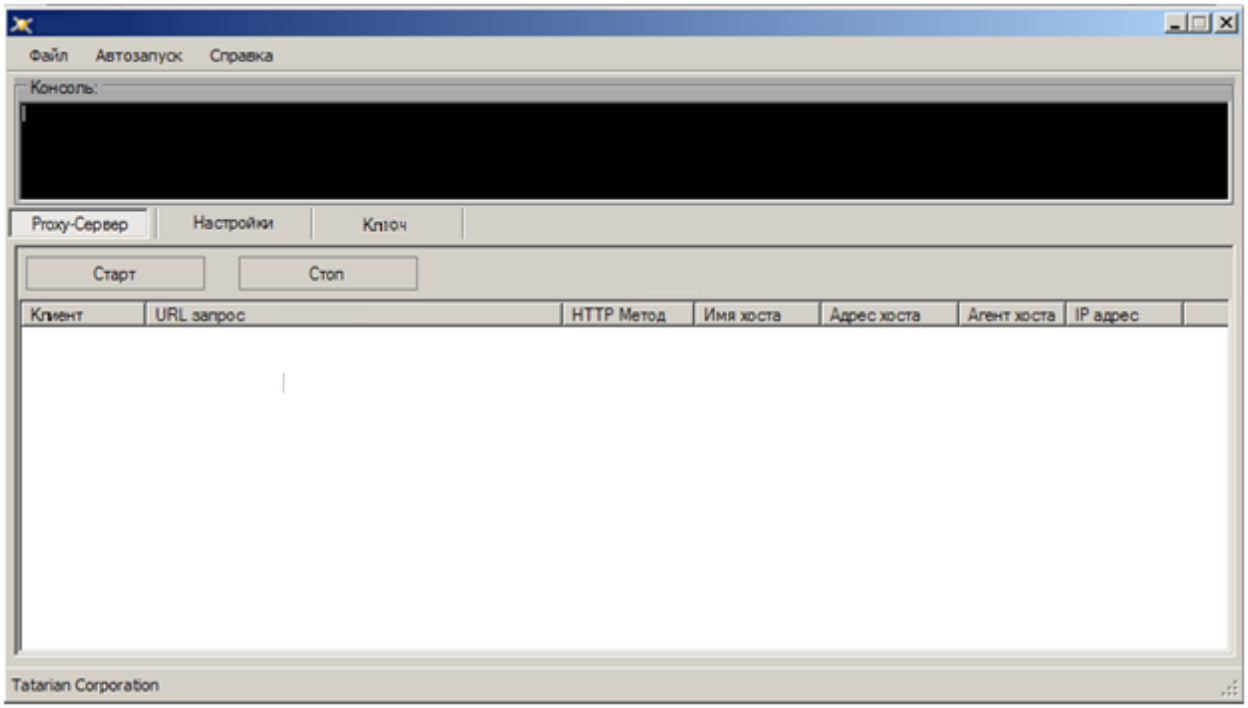

Рис. 6. Внешний вид программы

Далее будут даны определения каждому конфигурационному файлу. При запуске программы пользователю будет предоставлена на вид основная форма программы:

Форма состоит из следующих элементов:

– панели меню «Файл», «Автозапуск» и «Справка».
– консоли вывода «Консоль:», на которую выводятся системные сообщения работы программы.
– вкладок «Proxy-Сервер», «Настройки» и «Ключ».

«*Файл*» имеет единственную кнопку «Выход», при нажатии которой программа завершает свою работу и закрывается.

«*Автозапуск*» состоит из кнопок «*Включить*» и «*Выключить*». Если отмечена «Включить», то программа будет добавлена в автозагрузку и будет запускаться при запуске операционной системы. Если отмечено «Выключить», то, соответственно, программа будет убрана из автозагрузки.

Перед тем, как пользователи смогут начать пользоваться сервером, необходимо провести настройки программы на вкладке «*Настройки*».

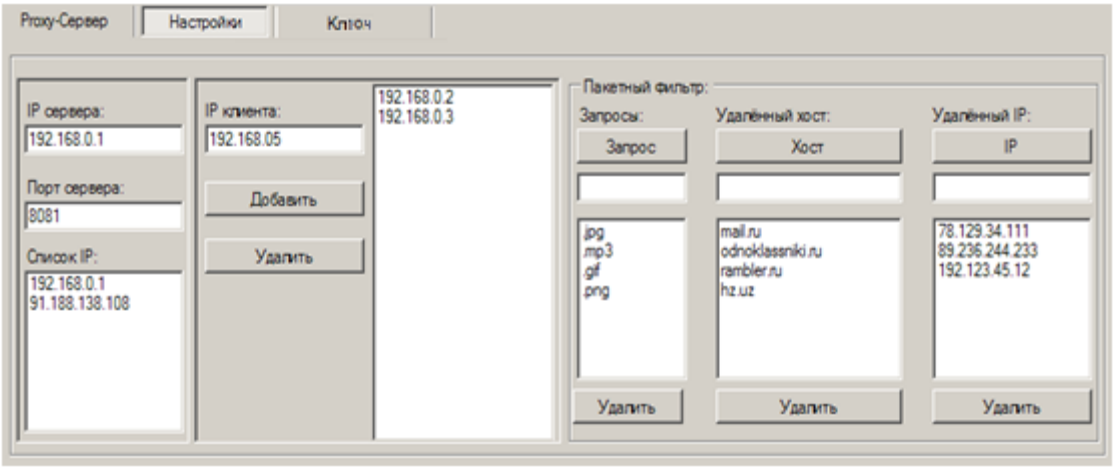

Рис. 7. Меню настройки программы

Вкладка «*Настройки*» состоит из 3 панелей:

– Настройка сервера:

- IP-сервера – IP-адрес, на котором будут прослушиваться запросы клиентов.
- Порт сервера – порт, который будет открыт для прослушивания на стороне сервера.
- Список IP – Список IP-адресов, которые присвоены серверу (зависит от количества сетевых адаптеров). Имеющиеся в списке IP можно выбрать для прослушивания двойным кликом на необходимом IP-адресе.

– Настройка клиентской части:

Текстовое поле «*IP-клиента*» – IP-адрес пользователя, которому будет разрешено пользоваться прокси-сервером.

Кнопка «*Добавить*» добавляет IP-адрес в список адресов, которым разрешено пользование услугами сервера, а также записывает в файл «proxyConfig.txt».

Кнопка «*Удалить*» удаляет IP-адрес из списка адресов и из файла «proxyConfig.txt».

– Панель пакетной фильтрации:

- программа позволяет фильтровать пользовательские запросы по содержанию запроса (например, можно запретить запрос, содержащий ".mp3", после чего, если пользователь захочет скачать mp3-файл, ему будет отправлено уведомление, что данный запрос невозможен из-за присутствия такого запроса в списке запрещенных запросов), по названию хоста(если в списке будет, например, mail.ru, то любой запрос к серверу mail.ru будет отклонен и пользователь будет уведомлен) и по удалённому IP (если IP-адрес, на котором располагается хост, который был задан в запросе пользователя, имеется в запрещенном

списке, то запрос будет отклонен и пользователь будет уведомлен).

Таким образом, программа имеет пакетную фильтрацию по критериям:

- Запросы (при добавлении запроса в запрещенный список, программа сохранит настройки в файл RawConfig.txt);
- Удалённый хост (при добавлении удалённого хоста в запрещенный список, программа сохранит настройки в файл HostConfig.txt);
- Удалённый IP (при добавлении IP-адреса в запрещенный список, программа сохранит настройки в файл IpConfig.txt);

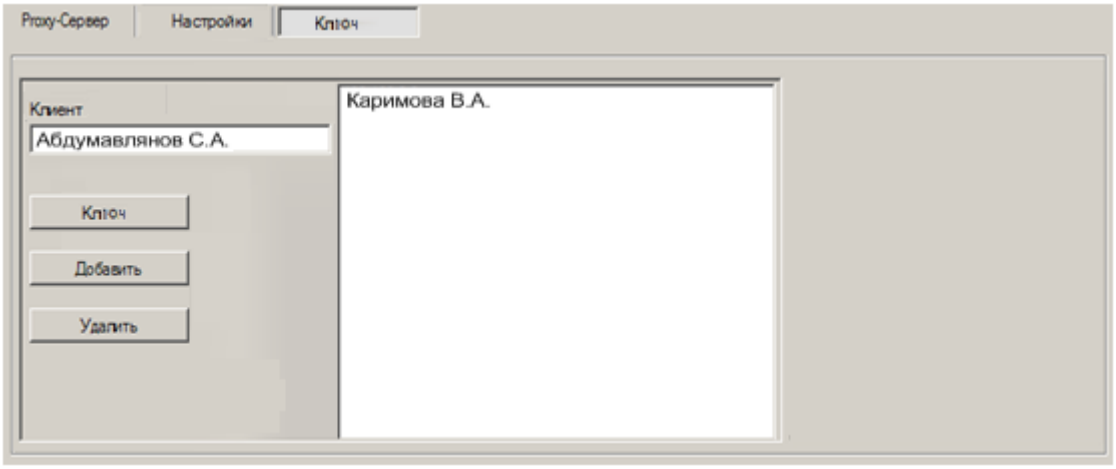

Рис. 8. Меню настройки ключа

Вкладка «*Ключ*» состоит из следующих панелей:

Текстовое поле «*Клиент*» – Идентификатор пользователя, которому будет разрешено пользоваться прокси-сервером.

Кнопкой «*Ключ*» указываем местоположения ключа.

Кнопка «*Добавить*» добавляет ключ пользователя в список которым разрешено пользование услугами сервера, а также записывает в файл «keyConfig.txt».

Кнопка «*Удалить*» удаляет ключ пользователя из списка и файла «keyConfig.txt».

Работа сервера начинается с нажатия кнопки «Старт» во вкладке «Proxy-Сервер», после чего будет выдана информация в Консоль:

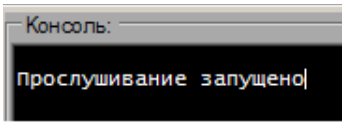

Рис. 9. Информирование администратора о запуске прослушивания портов.

Далее пользователю необходимо указать в настройках браузера параметры прокси-сервера(в данном случае IP-сервера - 192.168.0.1, порт – 8081) и попытаться открыть какую-либо web-страницу(в нижеследующем примере пользователь обращается по адресу mail.ru):

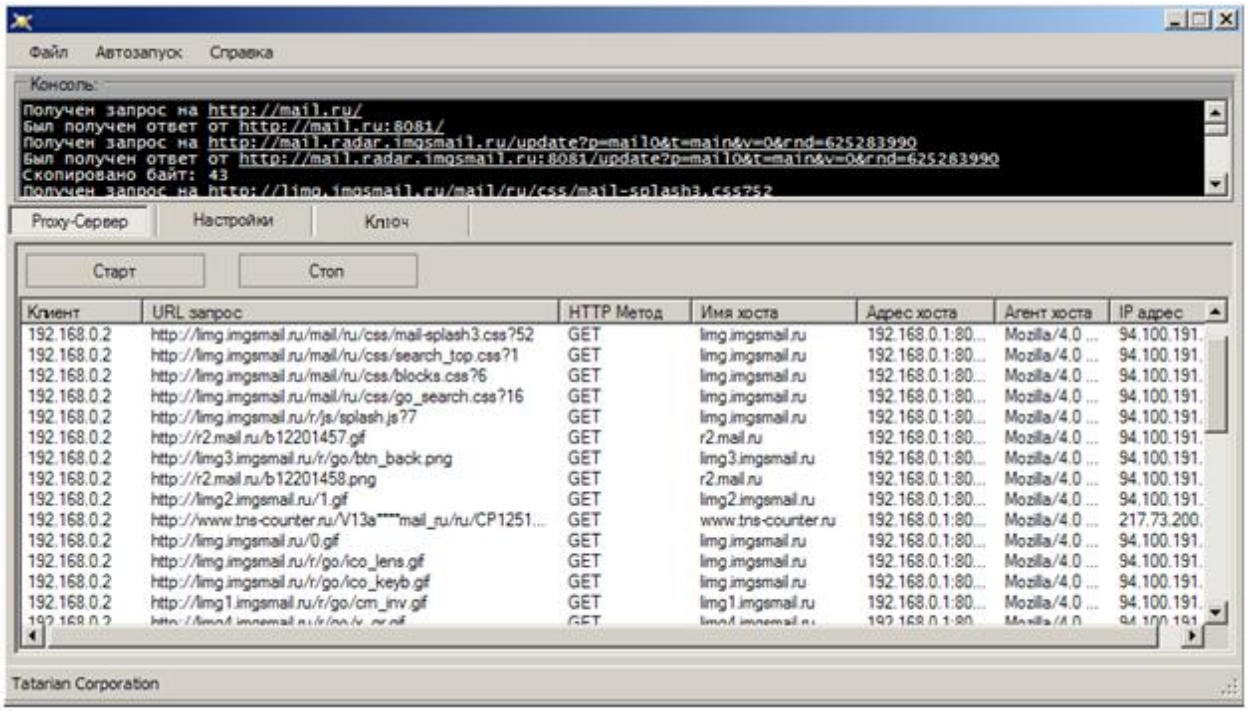

Рис. 10. Интерфейс программы во время обработки пользовательских запросов

Если IP-адрес пользователя имеется в списке разрешенных IP, то произойдет следующее:

- В Консоль выводится системная информация сервера. В информационной панели отображаются все действия пользователя(IP-адрес клиента, URL-запрос, HTTP-метод, имя хоста, адрес и порт сервера, агент хоста и IP-адрес, по которому располагается хост, указанный в запросе).

Если же IP-адрес клиента отсутствует в разрешенном списке, в консоли будет сообщено:

- «*Пользователь не имеет достаточных прав для пользования прокси-сервером*»
- Пользователь же на своей стороне получит в браузере ответ:
- «*Вы не имеете достаточных прав для пользования прокси-сервером*»
- Остановить прослушивание и работу сервера можно нажав «*Стоп*» на вкладке «Proxy-Сервер»:

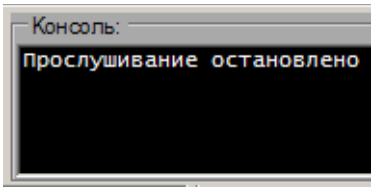

Рис. 11. Информирование администратора об остановке прослушивания портов.

Настройка компьютера пользователя, для работы через прокси-сервер. На предприятии необходимо чтобы все пользователи работали через пограничный межсетевой экран с функциями прокси-сервера.

Для настройки компьютера пользователей необходимо прописать в настройках интернет браузера IP-адрес и порт сервера, на котором ведётся ожидание подключений пользователей.

В данном случае, для примера настройки компьютера пользователя взят интернет браузер Mozilla Firefox 4.0.

Для указания IP-адреса и порта сервера необходимо пройти в настройки сети (Инструменты / Настройки/ Дополнительные / Сеть), кликнуть на панели «*Соединение*» кнопку «*Настроить*»:

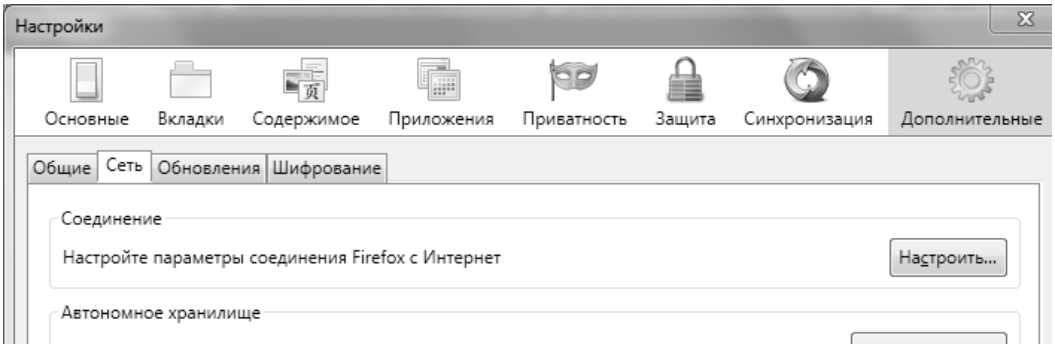

Рис. 11. Меню «Настройки» интернет браузера Mozilla Firefox 4.0

Прописать IP-адрес и порт сервера, на котором ведётся прослушивание:

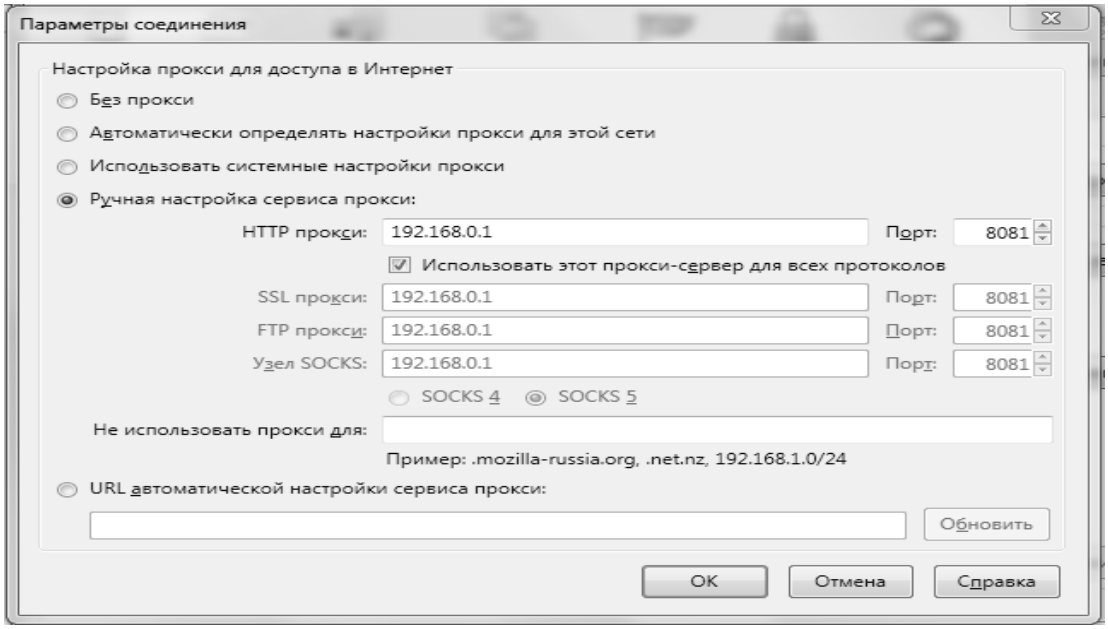

Рис. 12. Меню настроек параметров соединения интернет браузера Mozilla Firefox 4.0

В данном примере:

IP-адрес – 192.168.0.1

Порт – 8081

После применения настроек пользователь будет работать с внешней сетью только через пограничный прокси-сервер, и при попытке доступа на ресурс, находящийся в запрещенном списке, загрузка сайта будет приостановлена и пользователь будет получать сообщение, что данный ресурс находится в списке запрещенных ресурсов.

Аналогично будет срабатывать фильтр по содержимому запроса и по IP-адресу назначения, выдавая сообщение пользователю о блокировании ресурса.

Выводы по третей главе

1. Для разработки межсетевого экрана с классом фильтрации пакетов необходимо использовать методы, позволяющие просматривать содержимое пакетов информации, проходящих через межсетевой экран, одновременно не нарушая целостность и сохранность данных в этих пакетах.

2. В разработанном программном обеспечении, пользуясь которым можно на практике видеть работу межсетевого экрана с пакетной фильтрацией. В программу входит фильтрация запросов клиентов по содержимому запроса, по IP-адресу назначения и адресу хостов. Администратор может просматривать в журнале событий посещаемые в реальное время пользователями страницы.

Заключение

В данной диссертационной работе были рассмотрены межсетевые экраны и криптографические средства разработан программный модуль межсетевого экрана использующий аутентификацию на основе ключей для ограничения доступа в внутри сети

Межсетевых экран является основным элементом для обеспечения информационной безопасности в корпоративной сети позволяющий администратору сети централизованно осуществлять необходимую сетевую политику безопасности в выделенном сегменте сети. То есть, настроив соответствующим образом межсетевой экран, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящихся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Аутентификация пользователей является основной процедурой при проверке подлинность пользователей исходя из этого можно использовать специальные криптографические средства для аутентификации Межсетевые экраны делают возможной фильтрацию входящего и исходящего трафика, идущего через систему контролируя вместе с этим весь поток данных. Межсетевой экран использует один или более наборов «правил» для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Интегрирования модуля аутентификации на основе ключей в межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети. Они могут быть использованы для выполнения следующих задач:

Для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети Интернет.

Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети Интернет.

Для поддержки преобразования сетевых адресов (networkaddresstranslation, NAT), что позволяет использование во внутренней сети приватных IP-адресов (либо через один выделенный IP-адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

Список литературы

1. Постановление кабинета министров Республики Узбекистан «О мерах по созданию условий для дальнейшего развития компьютеризации и информационно-коммуникационных технологий на местах», (Собрание законодательства Республики Узбекистан, 2012 Г., № 5, ст. 47; 2013 г., №34, ст. 458).Г. Ташкент,1 февраля 2012 г.,№ 24.
2. Постановление кабинета министров Республики Узбекистан «О дополнительных мерах по повышению квалификации работников органов государственного и хозяйственного управления, государственной власти на местах в сфере информационно-коммуникационных технологий», (Собрание законодательства Республики Узбекистан, 2014 г., № 14, ст. 154).Г. Ташкент,27 марта 2014 г.,№ 73.
3. Постановление кабинета министров Республики Узбекистан «Об утверждении положения о порядке проведения изучения состояния внедрения и развития информационно-коммуникационных технологий в деятельности органов государственного и хозяйственного управления, государственной власти на местах», (Собрание законодательства Республики Узбекистан, 2014 г., № 17, ст. 195). Г. Ташкент, 23 апреля 2014 г.,№ 102.
4. Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А. Основы корпоративной теории информации. СПб: СПбГУ ИТМО, 2004
5. Гайкович В., Першин А. Безопасность банковских электронных систем, М.:1993
6. Скиба В.Ю., Курбатов В., «Руководство по защите от внутренних угроз информационной безопасности» - Издательство Питер, 2008 – 320 с.

7. Росенко А.П., «Внутренние угрозы безопасности конфиденциальной информации». Методология и теоретическое исследование, Издатель: «URSS (Красанд)» 2010 г.112 стр.

8. Костров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008 г. 226 стр.

9. Виснадул Б.Д., Лупин С.А., Сидоров С.В., Чумаченко П.Ю. Основы компьютерных сетей: Учеб. пособие.- М.: Форум: ИНФРА-М, 2007.- с.272.

10. Вишневский В.М. Теоретические основы проектирования компьютерных сетей.-М.: Техносфера, 2003. - с.512.

11. ГайдамакинН.А. Разграничение доступа к информации в компьютерных системах. Изд-во Уральского ун-та, 2003. - с.328.

12. Гмурман А.И. Информационная безопасность.- М.:БИТ-М, 2004 - с. 23-35.

13. Государственный стандарт Узбекистана. Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. 1-часть, Концепции и модели управления безопасностью информационно-коммуникационных технологий. O'zDStISO/IEC 13335-1: 2006.

14. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защиты информации: Учеб. для ВУЗов. М.:Машиностроение, 2009. - с. 508.

15. Крухмалев В.В., Гордиенко В.Н., Моченов А.Д., Иванов В.И., Бурдин В.А., Крыжановский А.В., Марыкова Л.А. Основы построения телекоммуникационных систем и сетей. - М.: Горячая линия - Телеком, 2004. - 510с.

16. Макконнелл Дж. Основы современных алгоритмов. 2 – е дополненное издание, М.: Техносфера, 2004. - с.368

17. Орлов С.А. Технологии разработки программного обеспечения. СПб: Питер, 2004.

18. Платонов В.В. Программно - аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для студ. ВУЗ, М.: Академия, 2006 - с.240

19. Сугак Е.В. и др. Надежность технических систем. – Красноярск: МГП РАСКО, 2008. - с.235.

20. Хорошко В. А., Чекатков А.А. Методы и средства защиты информации. – Киев: Юниор, 2003. - 270 - с.286.

21. Шангин В.Ф. Информационная безопасность компьютерных систем и сетей: Учеб. пособие. – М.: Форум: ИНФРА-М, 2010 - с.416.

22. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа.– СПб: Наука и техника, 2008. - с.383.