на правах рукописи

Томилин Василий Николаевич

РАЗРАБОТКА МЕТОДОВ АУТЕНТИФИКАЦИИ УЗЛОВ РАСПРЕДЕЛЕННОЙ IP-СЕТИ

Специальность: 05.13.19 – «Методы и системы защиты информации и информационной безопасности»

Автореферат диссертации
на соискание ученой степени
кандидата технических наук

Санкт-Петербург
2002

Работа выполнена в Санкт-Петербургском государственном политехническом университете.

Научный руководитель:

Доктор технических наук, профессор Зегжда П.Д.

Официальные оппоненты:

Доктор технических наук, профессор Корниенко А.А.
Кандидат технических наук, старший научный сотрудник Карпов А.Г.

Ведущая организация: Государственный университет телекоммуникаций

Защита состоится 21 ноября 2002 г.

в ____ часов на заседании диссертационного совета _____ Санкт-Петербургского государственного политехнического университета (по адресу 194021, Политехническая ул. 29/1, ауд.).

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского государственного политехнического университета.

Автореферат разослан “___” _____ 2002 г.

Ученый секретарь
диссертационного совета Платонов В.В.

Общая характеристика работы.

Актуальность. Распространение применения распределенных систем, обусловленное развитием вычислительной техники, сопровождается ростом количества абонентов распределенных вычислительных систем. Высокая квалификация не является естественным ограничителем количества пользователей, в результате рост количества абонентов носит экспоненциальный характер. Развитие автоматических и автоматизированных средств взаимодействия между узлами распределенной вычислительной системы обеспечивает простоту разрушительных воздействий на удаленные узлы. Для оказания разрушающего воздействия на удаленную систему злоумышленнику достаточно загрузить из сети готовое программное средство и указать цель разрушающего воздействия. В результате безопасность узлов сети часто нарушается лицами, профессионализм которых не позволяет им адекватно оценивать свои действия. Зачастую трудно обеспечить действенную защиту узла сети от действий удаленных пользователей; дополнительным средством, позволяющим предотвратить массовые нарушения безопасности, может стать система аутентификации удаленных абонентов сети.

В настоящее время самый распространенный протокол сетевого уровня, использующийся в распределенных сетях – IP (версии 4), не предоставляет средств аутентификации удаленного клиента или сервера. Средства аутентификации, заложенные в архитектуру протокола IP следующей версии, IPv6, также недостаточно развиты, кроме того, скорость распространения IPv6 ограничена. В то же время задача подделки адреса отправителя сетевого пакета не представляет сложности для программиста средней квалификации, что является предпосылкой к проведению ряда удаленных разрушающих воздействий со стороны клиента.

Проблема предотвращения удаленных разрушающих воздействий широко рассматривалась в работах специалистов в области информационной безопасности (Грушо А.А., Ухлинов Л.М., Лукацкий А.Д., Щербаков А.Ю, Белловин С., Спаффорд Ю., Чезвик М.). Попыткой «стандартизации» мер противодействия анонимной отправке IP-пакетов стал рекомендательный документ RFC 2827 “Network Ingress Filtering”, имеющий статус «описание рекомендуемых мероприятий» (Best current practice), но, к сожалению, необязательный к исполнению. Как следствие, на практике его требования часто игнорируются.

Таким образом, распределенная IP-сеть в настоящее время представляет собой систему, пользователи которой могут оказывать деструктивные воздействия на удаленные узлы, оставаясь практически анонимными. В такой системе представляется актуальной разработка системы аутентификации узлов сети на сетевом уровне сетевой модели.

Другим аспектом работы в распределенной сети, напрямую характеризующим безопасность взаимодействия, является возможность установления подлинности удаленного сервера. До сегодняшнего дня при решении задачи установления подлинности удаленного сервера, как правило, используются различные криптографические средства. Существующие криптографические методы успешно обеспечивают решение задачи установления подлинности удаленного сервера в большинстве случаев.

Тем не менее, в некоторых случаях использование криптографических средств неудобно для пользователей или не обеспечивает должной степени безопасности. Зачастую функционирование криптографических средств основано на использовании секретных данных, сохранность которых, в общем случае, не гарантирована. В данной ситуации существует вероятность компрометации секретных данных, хранящихся на сервере, что приводит к возможному нарушению безопасности клиента, доверяющего серверу. Кроме того, алгоритмы работы криптографических механизмов, зачастую, требуют регистрации клиентов в централизованном каталоге, что не позволяет использовать их для массового обслуживания незарегистрированных клиентов при работе в сети, безопасность которой не гарантирована.

Таким образом, на сегодняшний день актуальна задача аутентификации удаленных узлов сети (как клиентов, так и серверов).

Целью работы является разработка методов и средств аутентификации удаленных узлов сети в случае невозможности применения криптографических методов.

Для достижения поставленной цели в работе решались следующие задачи:

1. Систематизация использующихся в настоящее время методов аутентификации удаленных узлов сети.
2. Формализация постановки задачи разработки методов и средств аутентификации удаленного клиента.
3. Разработка методов и средств аутентификации удаленного клиента.
4. Формализация постановки задачи разработки методов и средств аутентификации удаленного сервера.
5. Разработка методов и средств аутентификации удаленного сервера.

Методы исследования. Для решения поставленных задач использовались теория алгоритмов, математическая логика, теория программирования, системный анализ и методы моделирования.

Научная новизна диссертационной работы состоит в следующем:

1. Предложена систематизация методов аутентификации удаленных узлов сети.
2. Разработаны методы и средства аутентификации клиентской части системы.
3. Разработаны методы и средства аутентификации серверной части системы.
4. Разработаны алгоритмы функционирования средств аутентификации клиентской и серверной частей системы.
5. Разработана методика создания дополнительных средств, необходимых для функционирования средств аутентификации удаленного клиента на основании протокола взаимодействия в ряде случаев.

Практическая ценность работы подтверждена тремя актами о внедрении предложенных в ней методов и полученных результатов для установления подлинности удаленного узла при различных сетевых взаимодействиях и обеспечения скрытной работы различных программных средств: от НИИ Системотехники х/к "Ленинец", в/ч 45187 и СПб филиала ГУП "Желдоринформзащита". Положения работы легли в основу учебных курсов, разработанных на кафедре Информационной безопасности Компьютерных систем СПбГПУ и ГУАП.

Основные положения, выносимые на защиту:

1. Формализованная постановка задачи разработки методов и средств аутентификации удаленных узлов сети.
2. Методы аутентификации клиентской части системы.
3. Методы аутентификации серверной части системы.
4. Методика создания дополнительных средств, позволяющих реализовывать скрытную работу средств аутентификации клиентской части системы.
5. Алгоритмы функционирования средств аутентификации удаленных узлов.

Публикации. По теме диссертации опубликовано 10 работ, в том числе 10 научных статей и докладов.

Объем и структура работы.

Диссертационная работа состоит из введения, четырех глав, заключения и списка литературы из 66 работ.

Содержание работы.

В первой главе рассматриваются цели и задачи аутентификации удаленного узла сети, проблемы, возникающие в ходе установления подлинности удаленного узла сети, существующие средства, решающие данную задачу. В главе рассмотрены возможные модели нарушителей, проведена систематизация способов аутентификации удаленного узла и сформулирована общая постановка задачи.

В данной работе под *аутентификацией* удаленного узла сети понимается набор действий, позволяющих установить, выполняется взаимодействие с заданным узлом сети или с другим узлом, выдающим себя за заданный узел. Например, аутентификация удаленного узла может заключаться в получении информации о подлинном сетевом адресе узла или о сегменте сети, в котором располагается узел, и сравнении полученной информации с предоставляемой узлом. При этом информация о сегменте актуальна для случая, когда удаленный узел не имеет сетевого адреса или не использует подлинный сетевой адрес в процессе работы в сети.

При решении задачи аутентификации узла сети рассмотрены две основные подзадачи – аутентификации клиентской и серверной части процесса сетевого взаимодействия. Для описания методов аутентификации удаленного узла сети рассмотрены возможные модели нарушителей.

При решении подзадачи аутентификации удаленного клиента используется разработанная соискателем неформальная модель нарушителя, описание которой представлено в табл. 1. При решении подзадачи аутентификации удаленного сервера предложены три другие неформальные модели нарушителя, представленные в табл. 1.

Таблица 1. Модели нарушителей при аутентификации клиента и сервера

Задача / Характеристика	**Аутентификация клиента**	**Аутентификация сервера**		
		Модель 1	**Модель 2**	**Модель 3**
Тип нарушителя	Активный	Активный	Активный	Активный
Расположение нарушителя	Распределенная сеть – любой сегмент	Сегмент атакуемого клиента	Промежуточный сегмент (не сегмент атакуемого клиента и не сегмент атакуемого сервера).	Сегмент удаленного сервера
Цель атаки	Сохранение анонимности	Подмена удаленного узла		
Способ реализации атаки	Искажение адресной информации об отправителе пакета	Ответы на запросы клиента от имени сервера		

Для реализации процедуры аутентификации удаленного узла в рамках работы решены следующие подзадачи:

1. Разработаны методы аутентификации клиента распределенной сети для принятой модели нарушителя.
2. Разработаны методы аутентификации сервера распределенной сети для принятых моделей нарушителей.

3. Разработаны специальные методы обеспечения функционирования средств аутентификации.

По результатам анализа методов аутентификации, применяемых в распределенных сетях, была разработана систематизация, представленная на рис. 1.

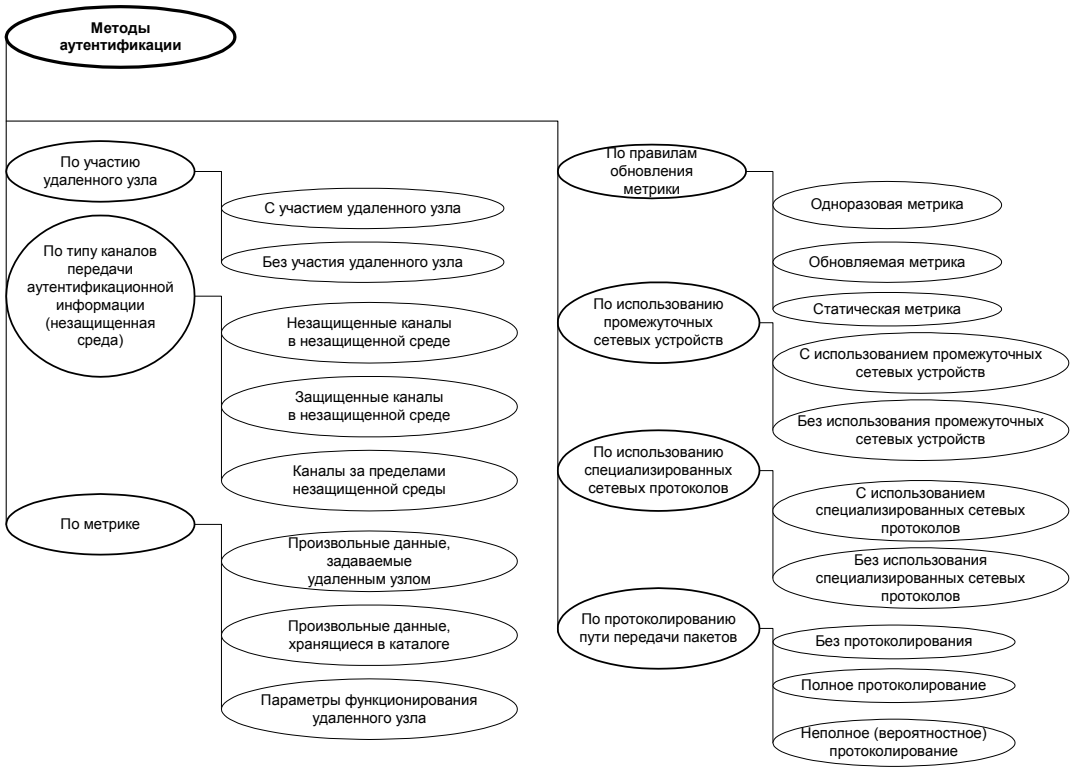

Рис. 1. Систематизация методов аутентификации удаленного узла распределенной сети

Для построения систем аутентификации удаленных узлов разработаны и реализованы следующие методы:

- при аутентификации удаленного клиента:
  - без участия удаленного узла;
  - использования незащищенных каналов передачи;
  - учета параметров функционирования удаленного узла;
- при аутентификации сервера:
  - с участием удаленного узла;
  - использования каналов передачи за пределами незащищенной среды
  - использования произвольных данных, задаваемых удаленным узлом.

На основе этих методов разработаны следующие системы аутентификации:

1. Аутентификация клиента на основании неполного (вероятностного) протоколирования с использованием промежуточных сетевых устройств;

2. Аутентификация сервера с использованием одноразовой метрики, произвольных данных, и каналов передачи секретной информации за пределами среды.

Во второй главе рассматривается создание системы аутентификации клиента на основе метода неполного протоколирования с использованием промежуточных сетевых устройств. Разработка системы аутентификации требует учета следующих функциональных особенностей IP-сетей:

1. удаленные узлы имеют возможность посылать произвольные IP-пакеты;
2. в сети не гарантируется доставка информации;
3. возможность функционирования незарегистрированных в ней узлов;
4. возможность передачи данных аутентифицируемым узлом;
5. соблюдение стандартов функционирования IP-сетей.

Задача аутентификации удаленного клиента формулируется в работе следующим образом: клиент, находящийся в одной подсети распределенной сети, осуществляет передачу данных на сервер, расположенный в удаленной подсети этой сети. Система аутентификации клиента реализует механизмы, позволяющие узлам удаленной подсети удостовериться, что данные отправлены именно данным клиентом, или определить примерное местоположение узла, выдающего себя за клиента.

При решении задачи аутентификации удаленного клиента с использованием протоколирования маршрута передачи совокупность данных, поступающих на узел ***B*** в направлении от узла ***A***, описывается следующим образом:

$$A \rightarrow B: Data, ADDRINFO(A), R(A, B) \quad (1)$$

где ***A*** – проходящий процедуру аутентификации клиент, передающий данные; ***B*** – узел, принимающие данные; ***Data*** – данные, передаваемые узлом ***A***; ***ADDRINFO(A)*** – адресная информация, заносимая в пакеты узлом ***A***, ***R(A, B)*** – функция описания маршрута передачи.

Типовая задача аутентификации позволяет выполнять аутентификацию узла за счет секретных данных, передаваемых в среде передачи.

$$A \rightarrow B: Data, R'(среда\ передачи, \ldots) \quad (2)$$

Таким образом, поставленная задача вписывается в формальную задачу типовой аутентификации.

Для разработки системы аутентификации удаленного клиента во второй главе работы исследовались и решались следующие задачи:

1. Анализ существующих способов аутентификации удаленных узлов с использованием характеристик среды передачи;
2. Разработка структуры системы аутентификации;
3. Анализ и обоснование метрики (набора признаков), идентифицирующей удаленный узел при использовании характеристик среды передачи;

4. Исследование взаимосвязей метрики и структуры системы аутентификации узлов;
5. Построение функции, позволяющей принимать решение об успешности аутентификации удаленного клиента *A*.

В качестве функции, описывающей характеристики среды передачи, введена следующая функция, использующая вставку специальных пометок в пакеты в распределенной сети:

$$R(A,B) = F(S(A,B), W(A,B), TR, L(A,B)) \quad (3)$$

где ***A*** – проходящий процедуру аутентификации клиент, передающий данные; ***B*** – узел, принимающий данные; ***S(A,B)*** – множество узлов, помечающих пакеты от ***A*** к ***B***; ***W(A,B)*** – функция занесения пометок в пакеты от ***A*** к ***B***; ***TR*** – множество узлов, извлекающих пометки из пакетов; ***L(A,B)*** – пропускная способность каналов, по которым осуществляется передача информации от ***A*** к ***B***.

Разработанный метод включает в себя выделение узлов распределенной сети, через которые проходят пакеты; занесение в пакеты идентификационной информации с определенной вероятностью; сбор информации об узлах, через которые передавались пакеты; восстановление маршрута передачи пакета; определение соответствия маршрута передачи указанному адресу узла ***A***; принятие решение об аутентификации узла ***A***.

Введенная функция (3) послужила основой для разработки структуры системы аутентификации удаленных сетевых узлов.

При разработке структуры системы аутентификации удаленных сетевых узлов были решены следующие задачи:

1. Определен состав системы аутентификации удаленных узлов. В распределенной сети в состав системы аутентификации входят:
   - узлы пометки пакетов, заносящие в передаваемые через них пакеты идентификационную информацию с определенной вероятностью (реализуют функцию ***W(A, B)***);
   - модули сбора идентификационной информации, выполняющие сбор идентификационной информации, занесенной в пакеты узлами пометки пакетов, анализ собранной информации (реализуют ***R(A,B)***) и сопоставление маршрута передачи ***R(A,B)*** с адресной информацией ***ADDRINFO(A)*** для принятия решения об аутентификации клиента (реализуют функцию ***AUTH[R(A,B), ADDRINFO(A)]***).
2. задано расположение компонентов системы аутентификации удаленных узлов в распределенной сети с учетом следующих ограничений:
   - расположение компонентов системы определяет объем и формат идентификационной информации, которая должна быть занесена в пакеты. В частности, включение идентификационной информации в сетевые пакеты требует перерасчета контрольных параметров сетевых пакетов.

- Расположение компонентов системы аутентификации определяет «направленность» системы. Так, контроль одного высокоскоростного канала и пометка пакетов, передаваемых по нему, не обеспечит получателя идентификационной информации сведениями об узлах, подключенных к низкоскоростному каналу передачи информации, из которого был передан данный пакет.

Основным элементом разработанной системы аутентификации являются, так называемые, узлы пометки пакетов, которые размещаются на сетевых устройствах, обслуживающих периферийные сетевые каналы, т.е. на таких устройствах, производительность которых позволяет выполнять полную обработку сетевого пакета, включая перерасчёт контрольной суммы.

При заданном максимально допустимом времени обработки (***MWT***) для узла пометки пакетов справедливо следующее выражение

$$W(A,B) = F(MWT, L(A,B)). \quad (4)$$

Формат передачи метрики узла определяется максимально допустимым временем обработки пакета и способом кодирования метрики. Для обеспечения совместимости с существующими сетями передачи данных при определении формата передачи данных, используемых для аутентификации узла, соблюдались стандартные форматы пакетов; для обеспечения функционирования системы рассматривалась возможность обнаружения информации, связанной с аутентификацией, на промежуточных узлах.

В работе предложен и реализован способ передачи идентификационной информации с использованием опции IP-заголовка.

Важным элементом системы аутентификации удаленного клиента являются узлы сбора идентификационной информации для решения задачи восстановления маршрута. Решение данной задачи выполняется модулем сбора идентификационной информации в три этапа:

1) накопление информации;
2) анализ достаточности накопленной информации;
3) восстановление маршрута.

В процессе выполнения работы соискателем разработаны алгоритмы для восстановления маршрута для различных вариантов метрик:

- метрика, идентифицирующая один узел пометки пакетов,
- метрика, идентифицирующая один узел пометки пакетов, а также расстояние до него от узла отправителя пакетов,
- метрика, идентифицирующая два узла пометки пакетов и расстояние между ними.

Исходными данными для алгоритма решения задачи восстановления маршрута являются поступившие в сетевых пакетах метрики, составленные различными узлами пометки пакетов. Задача восстановления маршрута состоит в формировании фрагментов маршрута, достаточных для его анализа, для случая, когда метрика содержит сведения о расстоянии между узлами пометки пакетов, и в формировании набора узлов, через которые передавались пакеты, в противном случае.

Например, при восстановлении маршрута для метрики, идентифицирующей два узла пометки пакетов и расстояние между ними, отрезки маршрута формируются в виде последовательностей пар $\{N_i, d_i\}$, где N – адрес узла пометки пакетов, а d – расстояние до узла N от узла, представляющего собой начало фрагмента маршрута, в который входит узел N. Упорядочивание выполняется по возрастанию d. Результатом восстановления маршрута является набор фрагментов маршрута.

Исходным множеством узлов называются такие узлы, адреса которых были получены модулями сбора идентификационной информации в составе идентификационных меток пакетов.

Алгоритм восстановления маршрута передачи пакетов включает в себя следующие шаги:

1. В начале алгоритма "множество узлов, путь до которых известен", принимается за пустое.
2. Включить в множество узлов, путь до которых известен, узел-получатель пакетов.
3. Выделить из исходного множества те узлы пометки пакетов, расстояние до которых измеряется от узлов, входящих в "множество узлов, путь до которых известен".
4. Если множество выделенных узлов не пусто, поместить их в соответствующие им точки последовательностей. Включить такие узлы в "множество узлов, путь до которых известен" (расстояние до добавляемого узла равняется сумме расстояния до добавляемого узла от узла, путь до которого известен, и расстояния от узла-получателя пакетов до узла, путь до которого известен). Удалить добавленные узлы из исходного множества.
5. Если множество выделенных узлов пусто, а исходное множество не исчерпано, то считать восстановленным очередной фрагмент маршрута, зафиксировать упорядоченную последовательность ребер, его составляющих, удалить все элементы множества узлов, путь до которых известен, выбрать случайный узел из исходного множества и включить его в "множество узлов, путь до которых известен". При этом расстояние от узла-получателя пакетов до вновь добавленного узла не определяется, вычисление расстояний до узлов, связанных с вновь добавленным узлом, ведется относительно вновь добавленного узла.

6. Пока не исчерпано все исходное множество, повторять шаги ***3***, ***4***, ***5***.

При размещении компонентов системы на низкоскоростных каналах передачи информации необходимо обеспечить скрытную работу компонентов системы от типовых средств администрирования узла вычислительной сети (если средства аутентификации функционируют без ведома владельца узла сети). Для решения вопросов обеспечения скрытности в работе были проанализированы и решены следующие основные задачи:

1. систематизация методов обеспечения скрытности от средств административного контроля;
2. методика обеспечения скрытности от утилит административного контроля.

Разработанная в работе систематизация методов обеспечения скрытности приведена на рисунке 2.

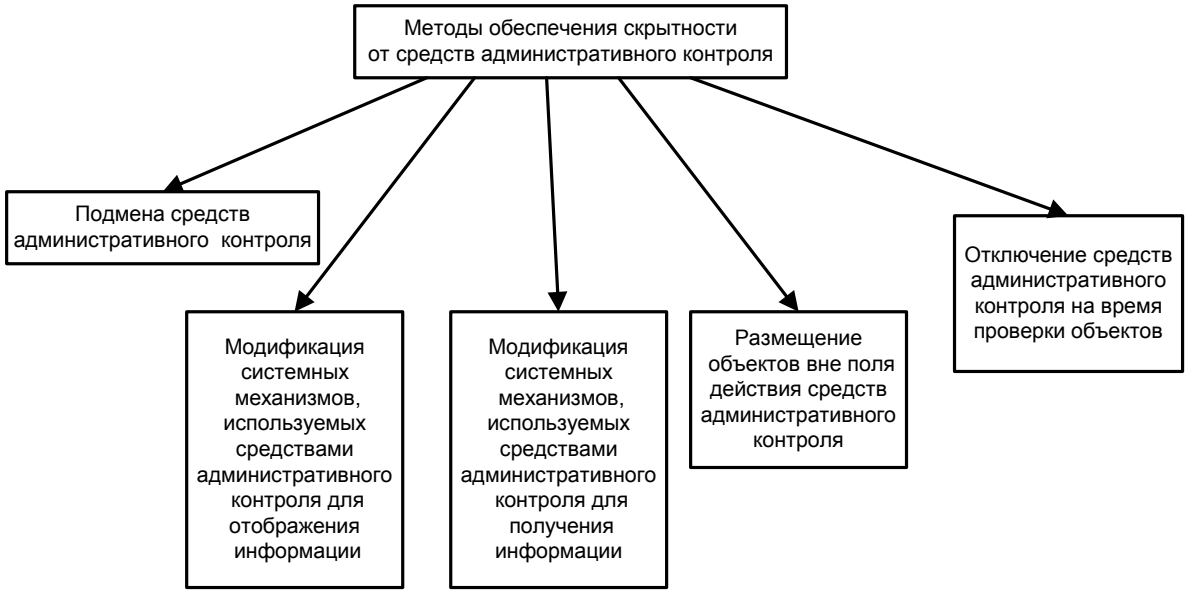

Рис. 2. Систематизация методов обеспечения скрытности объектов операционной системы от средств администрирования

В результате анализа различных методов обеспечения скрытности объектов от средств административного контроля, проведенного в ходе выполнения работы, выбран метод модификации системных механизмов, используемых средствами административного контроля для получения информации.

Алгоритм методики обеспечения скрытности объектов операционной системы от средств административного контроля состоит из следующих этапов:

1. Определить тип узла и средства административного контроля, функционирующие на нем.
2. Выбрать средства административного контроля, защиту от которых необходимо обеспечить.

3. Множество модифицируемых системных механизмов принять за пустое.
4. Для всех выбранных средств административного контроля выполнять шаги ***5***, ***6***, *7*.
5. Определить системные механизмы, используемые в работе средства административного контроля.
6. Проанализировать возможность вмешательства в работу системных механизмов, используемых в работе средства административного контроля. Если вмешательство возможно, то перейти на шаг *7*. В противном случае перейти к следующему механизму, используемому в работе данного средства. Если перебраны все системные механизмы, используемые в работе средства административного контроля, и обеспечить вмешательство в их работу невозможно, принять решение о невозможности обеспечить скрытность от данного средства административного контроля.
7. Добавить системный механизм в множество модифицируемых системных механизмов. Если для одного средства административного контроля существует возможность модификации нескольких системных механизмов, то следует использовать те механизмы, которые уже включены в множество модифицируемых системных механизмов.
8. Модифицировать работу системных механизмов для фильтрации данных о скрываемых объектах операционной системы для средств административного контроля.

В процессе научно-исследовательской работы по тематике диссертации, соискателем были разработаны и описаны во второй главе практические средства обеспечения скрытности основных объектов операционных систем (в частности Linux и FreeBSD), таких как: файлы, процессы и т.п.

В третьей главе рассматривается задача аутентификации удаленного сервера в распределенной сети. В этом случае задача нарушителя состоит в имитации удаленного сервера для клиента распределенной сети. Рассмотрены три модели нарушителя, выдающего себя за удаленный узел сети, причем допускается, что нарушители могут располагать любыми данными, использующимися для аутентификации сервера, которые хранились на сервере или к которым сервер имел доступ перед взаимодействием клиента и сервера. Кроме того, нарушители имеют возможность прослушивать сетевой трафик, блокировать передачу сервером информации, используемой при аутентификации, или подменять ее. По результатам проведенных исследований решения поставленной задачи, была разработана система, позволяющая проводить аутентификацию сервера, но не предназначенная для обеспечения безопасности канала передачи информации.

В ходе выполнения работы разработана система, позволяющая множеству удаленных клиентов удостоверяться в подлинности множества удаленных серверов.

Процесс взаимодействия клиента и сервера при аутентификации удаленного сервера описывается следующим образом:

$$A \rightarrow B: DataA;\ B \rightarrow A: Resp(DataA);$$
$$A: AUTH(DataA, R(DataA)) = \{0,1\} \quad (5)$$

где ***A*** – клиент, передающий данные; ***B*** – проходящий процедуру аутентификации сервер, принимающий данные; ***DataA*** – запрос клиента серверу; ***Resp(DataA)*** – функция построения ответа сервера; ***AUTH(DataA, R(DataA))*** – функция аутентификации сервера.

В ходе решения поставленной задачи был разработан следующий протокол взаимодействия клиента и сервера:

1. Установление клиентом соединения с сервером по независимому каналу передачи информации, неподконтрольному для нарушителя.
2. Передача клиентом серверу контрольного вопроса и правильного ответа на него (парольной информации). Если независимый канал передачи информации обеспечивает при этом обратную связь, то сообщение от клиента серверу должно включать в себя идентификатор клиента для обратной связи.
3. При обращении к серверу по глобальной сети (с использованием стандартного канала связи) клиент передает контрольный вопрос и, если это возможно, идентификатор клиента. Далее получает от сервера ответ и сравнивает его с правильным ответом на вопрос, переданным ранее на сервер по неподконтрольному каналу связи (см. п.2).
4. Если ответ, полученный от сервера по стандартному каналу связи, совпадает с ответом, переданным на сервер по неподконтрольному каналу связи, то подлинность сервера считается установленной.

Реализация данного протокола обеспечивается функцией создания независимого канала связи Θ:

$$\Theta(\mathbf{a}, \mathbf{b}): \forall\ c \in C, \forall\ s \in S\ \exists\ \Theta(c, s) \quad (6)$$

где C – множество клиентов, S –множество серверов.

В ходе построения системы аутентификации удаленного сервера были определены и решены следующие подзадачи:

- Анализ вариантов организации независимых каналов связи между сервером и клиентом.
- Анализ служб каталога (координат серверов), позволяющих множеству клиентов создавать независимые каналы связи с множеством серверов.
- Разработка формата хранения информации в службе каталога.
- Анализ средств взаимодействия клиента со службами каталога.

- Разработка средств выдачи сообщений в независимый канал связи на стороне клиента и средств автоматического извлечения сообщений на стороне сервера.
- Разработка форматов сообщений, передаваемых между клиентом и сервером.

В процессе анализа возможных вариантов организации независимых каналов связи соискателем были сформулированы следующие требования к независимому каналу передачи парольной информации:

1. Обеспечение конфиденциальности передаваемых сообщений.
2. Доставка сообщений за ограниченный интервал времени.
3. Возможность подтверждения доставки сообщения.
4. Экономическая целесообразность создания канала для массового пользователя.
5. Использование среды передачи, отличной от среды передачи канала передачи основной информации.
6. Обработка парольной информации, поступающей на сервер по каналу, в автоматическом режиме.

Одним из таких каналов, рассмотренных в процессе анализа существующих систем связи, является служба передачи коротких текстовых сообщений (SMS, Short Message Services) стандарта сотовой связи GSM, которая удовлетворяет сформулированным в работе требованиям.

В ходе решения задачи создания службы каталога, обеспечивающего предоставление координат удаленного сервера удаленному клиенту по запросу последнего, было установлено, что клиент при работе в распределенной сети с множеством ресурсов, как правило, использует услуги стандартной базы данных DNS. Поэтому для преобразования уникального идентификатора расположения ресурса (URL) в соответствующий телефонный номер мобильного телефона соискателем была разработана и предложена новая запись ресурсов DNS ***CP*** (от ***Cell Phone***). Это позволяет использовать в качестве каталога уже существующий механизм DNS, в который вводится дополнительная запись ресурсов. Данный подход облегчает решение задачи передачи запросов к службе каталога, поскольку в этом случае обращение клиента к каталогу выполняется как запрос клиента DNS-серверу с использованием существующей структуры DNS-запроса, а в качестве типа записи ресурсов указывается ***CP***.

Для решения задачи разработки средств передачи и приема сообщений были исследованы и проанализированы следующие способы отправки коротких текстовых сообщений в распределенных сетях:

- Использование мобильного телефона.
- Использование систем двунаправленной передачи сообщений с аутентификацией отправителя.
- Использование систем однонаправленной передачи сообщений.

В результате исследований было установлено, что для проведения аутентификации сервера отправитель может пользоваться любым из перечисленных способов передачи сообщений. Выбор способа передачи SMS определяется техническим оснащением клиента, моделью нарушителя и необходимостью получать подтверждение доставки SMS (см. табл. 2).

Таблица 2. Возможность осуществления аутентификации сервера в зависимости от модели нарушителя и оснащенности клиента

Модель нарушителя Оснащение клиента	**Модель 1**	**Модель 2**	**Модель 3**
Мобильный телефон	Аутентификация возможна	Аутентификация возможна	Аутентификация возможна
Система двунаправленной передачи сообщений	Аутентификация невозможна	Аутентификация вероятна	Аутентификация возможна
Система однонаправленной передачи сообщений	Аутентификация невозможна	Аутентификация вероятна	Аутентификация возможна

Значение «Аутентификация вероятна» в табл.2 указывает на то, что существует ненулевая вероятность перехвата злоумышленником информации, использующейся при аутентификации, поэтому использование соответствующего способа отправки сообщений является нежелательным.

Прием коротких текстовых сообщений осуществляется мобильным телефоном, подключенным к серверу через интерфейсный кабель; обработка принятых сообщений осуществляется программными средствами, разработанными соискателем в ходе проводимых исследований.

В ходе построения системы аутентификации удаленного сервера были разработаны форматы сообщений, передаваемых между клиентом и удаленным сервером, а именно SMS, передаваемые между клиентом и сервером, и сообщения протоколов распределенной сети.

В разработанном формате, решающем задачу аутентификации, при использовании обратной связи сервера с клиентом в текстовое сообщение включаются:

- строка запроса в формате «**Q:<контрольный вопрос>**”, где длина поля контрольного вопроса не превышает 120 символов латинского алфавита;
- строка ответа в формате «**R:<правильный ответ>**”, где длина поля правильного ответа не превышает 120 символов латинского алфавита;
- идентификатор клиента (номер отправителя в формате E.164), передаваемый мобильным телефоном или системой двунаправленной передачи сообщений с аутентификацией отправителя.

При взаимодействии по каналам распределенной сети клиент и сервер используют существующие прикладные протоколы, которые дополняются набором сообщений, передаваемым в начале взаимодействия: от клиента серверу – **SMSID** “<идентификатор клиента>” и **SMSQ** “<контрольный вопрос>”. В случае, если короткое текстовое сообщение не содержало идентификатора клиента, в качестве идентификатора клиента указывается “NOT SPECIFIED”. От сервера клиенту – **SMSR** “<правильный ответ>”.

Поскольку контрольный вопрос и правильный ответ определяются пользователем, большое внимание уделено поведение системы аутентификации при совпадении контрольных вопросов. При случайном совпадении контрольных вопросов предложенная и реализованная система аутентификации сервера позволяет проводить аутентификацию неограниченного количества пользователей, указавших идентификатор и одного пользователя, не указавшего идентификатор (поскольку нет возможности различить пользователей, которые задали одинаковый контрольный вопрос и не указали идентификатор).

Разработанный алгоритм аутентификации удаленного сервера включает в себя следующие шаги:

1. Если не известен телефонный номер, на который следует передавать SMS для аутентифицируемого сервера, то определить его с использованием механизмов DNS.
2. Выбрать способ передачи коротких текстовых сообщений, исходя из данных табл.2.
3. Выбрать контрольный вопрос и правильный ответ на него.
4. Передать SMS сообщение, содержащее контрольный вопрос и правильный ответ на него, в соответствии с заданным форматом сообщения. Номер определен на шаге ***1***, канал передачи выбран на шаге ***2***.
5. Если выбранный канал передачи сообщений позволяет получить подтверждение доставки, дождаться подтверждения доставки сообщения с парольными данными.
6. При начале взаимодействия с удаленным сервером по каналам распределенной сети передать ему контрольный вопрос и идентификатор.
7. Ожидать ответ. Если ответ получен, и он совпадает с правильным ответом, переданным на сервер, то сервер считается прошедшим аутентификацию.

В четвертой главе рассматриваются практические вопросы создания средств аутентификации узлов распределенной сети, реализованных с использованием разработанных методик и алгоритмов.

В работе получены следующие основные результаты:

1. Проведена систематизация методов аутентификации удаленных узлов.

2. Формализована задача на разработку методов и средств аутентификации узлов.
3. Разработана система аутентификации удаленного клиента.
4. Разработана методика обеспечения скрытной работы компонентов системы аутентификации удаленного клиента.
5. Формализована задача на разработку методов и средств аутентификации удаленного сервера.
6. Разработана система аутентификации удаленного сервера.
7. Разработаны средства аутентификации удаленного сервера.

Основные результаты диссертации изложены в 10 печатных работах.

1. Томилин В.Н. Защита абонентов многосегментной IP-сети от межсегментных угроз с помощью промежуточных сетевых устройств, Тезисы докладов конференции «Проблемы информационной безопасности. Компьютерные системы», 1998, сс. 180-184.
2. Кудряшов В.Н., Томилин В.Н. Контроль безопасности корпоративной сети на основании системы обнаружения удаленных атак. «Проблемы информационной безопасности. Компьютерные системы», №3, 1999, сс. 85-93.
3. Томилин В.Н. Методы обнаружения атакующего при проведении атак отказа в обслуживании группы flooding. «Проблемы информационной безопасности. Компьютерные системы», № 3, 2000, сс. 43-47.
4. Томилин В.Н. Атаки отказа в обслуживании в IP-сетях. BYTE-Россия, № 11, 2000, сс. 68-72.
5. Томилин В.Н. Оценка применимости систем обнаружения нарушителя к обнаружению атак отказа в обслуживании. «Проблемы информационной безопасности. Компьютерные системы», № 4, 2000, сс49-54.
6. Томилин В.Н. Опосредованные распределенные удаленные атаки, «Проблемы информационной безопасности. Компьютерные системы», № 1, 2001, сс. 34-37.
7. Томилин В.Н. Создание интегральной системы профилирования удаленного узла распределенной сети. Информационная безопасность регионов России, 2001, тезисы докладов.
8. Томилин В.Н. Профилирование удаленного узла распределенной сети. Конференция МИФИ, 2001, тезисы докладов.
9. Томилин В.Н. Использование средств сотовой связи для создания дополнительных каналов передачи секретной информации. «Проблемы информационной безопасности. Компьютерные системы», № 3, 2002, сс. 60-62.
10. Жульков Е.В., Томилин В.Н. Поиск уязвимостей сетевых систем обнаружения вторжения. «Проблемы информационной безопасности. Компьютерные системы», № 4, 2002.