Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

**Выявление протоколов удаленного доступа**

КУРСОВАЯ РАБОТА

студента 3 курса 331 группы

специальности 10.05.01 «Компьютерная безопасность»

факультета компьютерных наук и информационных технологий

Енца Михаила Владимировича

Научный руководитель

профессор, к.ф.-м.н. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Гортинский

подпись, дата

Зав. кафедрой

профессор, к.ф.-м.н. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Н. Салий

подпись дата

Саратов 2017 г.

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ 3

1 Основные алгебраические конструкции 4

2 Деревья 7

3 Код Прюфера 10

4 Практическая часть 14

4.1 Построение плоского изображения дерева 14

4.2 Построение кода Прюфера 15

4.3 Построение плоского изображения дерева из кода Прюфера 16

ЗАКЛЮЧЕНИЕ 20

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 23

ПРИЛОЖЕНИЯ 24

**ВВЕДЕНИЕ**

В настоящее время эффективная работа, связанная с анализом и обработкой информации, невозможна без использования компьютерных сетей. Частные сети фирм сеть Интернет предоставляют доступ к базам данных и новостям (RSS). Кроме того, пользователь получает возможность коллективной работы и оперативных консультаций с коллегами и экспертами. Подобные услуги оказываются необходимыми для бизнесменов, врачей, учителей, госчиновников, журналистов и т.п. Для обеспечения такого рода работы в рамках некоторой структуры, например, фирмы, используют локальные сети.

Однако физическая реализация локальной сети не всегда возможна и/или удобна. Часто складывается ситуация, когда подразделения фирмы географически удалены друг от друга или работники находятся не в помещение офиса, а работают с клиентами на местах, выезжают в командировки. В этом случае важно организовать работу таким образом, чтобы, находясь в отдалении от локальной сети фирмы, они, тем не менее, могли подключиться к ней.

Для того чтобы обеспечить доступ к услугам локальной сети при отсутствии непосредственного подключения к ней, служат средства удаленного доступа к сети. Эти средства использую для связи удаленного компьютера с локальной сетью. Они обеспечивают передачу данных на любые расстояния.

В то же время не следует забывать о том, что данные в подобных системах передаются на большое расстояние и, часто, по сетям общего пользования, доступ к которым не ограничен.

Актуальность, безопасности передаваемых данных и их защиты от несанкционированного доступа в системах удаленного доступа требует особенно пристального внимания и применения специальных методик, которые гарантировали бы достаточную конфиденциальность и достоверность данных. В противном случае, хакер, подключившийся в качестве удаленного клиента или перехватывая трафик реально существующего клиента, сможет украсть данные являющееся коммерческой тайной или фальсифицировать их.

Задача, решаемая данной работой связана с решением обозначенной выше проблемы и может быть сформулирована следующим образом: Проанализировать и исследовать существующие способы обеспечения безопасности работы в системах удаленного доступа и выработать рекомендации по выбору конкретного способа.

1. **Методы и средства удаленного доступа.**

Под средствами удаленного доступа понимаются средства, необходимые для связи небольших локальных сетей и даже удаленных отдельных компьютеров с центральной локальной сетью предприятия. В качестве отдельных удаленных узлов могут также выступать банкоматы или кассовые аппараты, требующие доступ к центральной базе данных о легальных клиентах банка, пластиковые карточки которых необходимо авторизовать на месте. Банкоматы или кассовые аппараты обычно рассчитаны на взаимодействие с центральным компьютером по сети Х.25, которая в свое время специально разрабатывалась как сеть для удаленного доступа неинтеллектуального терминального оборудования к центральному компьютеру.

Методы удаленного доступа.

Метод удаленного доступа – это метод, при котором пользователь удаленного терминала с помощью специального программного обеспечения подключается по глобальной сети к другому компьютеру, как локальный узел. Этот способ часто используется на мини-компьютерах, но мало распространен в ЛВС. Удаленной управление (remote control) – это метод, который позволяет удаленному пользователю получить контроль над локальными ПК в ЛВС корпорации (т. е. управлять одним из ПК в ЛВС). Скорость проведения сеанса и его возможности зависят от характеристик управляемого ПК, т. к. именно на нем выполняется обработка всех сетевых команд. Коды клавиш, нажимаемых на удаленном ПК, посылаются в управляемый ПК, а все изменения на экране управляемого выводятся на экран удаленного ПК Удаленное управление Используемые файлы и прикладные программы не загружаются в удаленный ПК. Передача через модем со скоростью 2400 – 57600 бит/с. Недостаток метода: для выполнения одной работы задействованы два ПК. Метод удаленного узла (remote node) основан на использовании сервера удаленного доступа, который служит своего рода «регулировщиком» и позволяет отдельному удаленному ПК или ЛВС связываться с центральной ЛВС. Программное обеспечение удаленного ПК, реализующее функции удаленного узла, позволяет ему функционировать как полноценному пользователю ЛВС. Как только связь установлена, телефонные линии становятся «прозрачными» и пользователь может работать со всеми ресурсами сети, как будто он сидит за ПК, непосредственно подключенным к ЛВС. Сервер удаленного доступа может быть реализован: в виде модема со встроенным специальным ПО; либо быть сервером ЛВС, на котором выполняются программы удаленного узла желательно, чтобы на удаленном ПК помимо сетевого системного ПО находилось все прикладное ПО, необходимое для сеанса связи: все выполняемые (\*.exe) файлы; необходимые Windows-приложения. В противном случае их необходимо будет передавать с сетевого сервера на канал связи. Т. к. они имеют, как правило, большие объемы данных, то это потребует значительных затрат времени. Удаленный узел как каждый полноценный пользователь ЛВС, удаленный узел имеет свой сетевой адрес. Сетевая операционная система преобразует сетевые пакеты, которые нужно передать через модем, из формата протокола IP или IPX в формат, совместимый со стандартом последовательной передачи. С появлением все большего количества программ, поддерживающих архитектуру «клиент - сервер», усиливается тенденция на программное обеспечение для удаленных узлов, т. к. такие программы позволяют обрабатывать большие файлы данных на серверах ЛВС, а на удаленный ПК передать только результаты обработки.

**1.1 Программы удаленного администрирования**

Для реализации удаленного доступа к ЛВС существуют более десятка известного ПО. В операционных системах семейства Windows существует встроенный помошник для реализации удаленного доступа. Для его запуска нужно выполнить команду «mstsc». В появившимся окне делаем нужные настройки (параметры экрана, звука и так далее), вводите имя компьютера и имя пользователя, под которым вы должны зайти. Нажимаете кнопку "Подключить", после чего, если компьютер будет найден и подключение возможно, у вас запросят пароль пользователя. Эти данные можно сохранить, чтобы в следующий раз подключаться без ввода пароля.

Часто требуется удаленное подключение к системам с разными операционными системами и здесь встроенный мастер Windows не поможет.

Однако для протокола, который используется в мастере удаленных подключений Windows – RDP (о нем ниже), реализации существуют практически для всех версий Windows (включая Windows CE, Phone и Mobile), Linux, FreeBSD, Mac OS X, iOS, Android, Symbian.

Для обхода этой проблемы можно использовать стороннее ПО, например, Radmin, TeamViewer, Ammy admin и т.д.

Каждая из этих программ предоставляет удобный интерфейс для реализации удаленного доступа.

Рассмотрим подробнее работу программы AeroAdmin:

При запуске программы открывается главное окно (рис. 1)

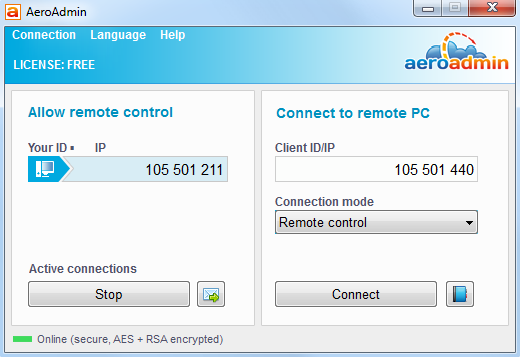


Рис. 1 Главное окно программы AeroAdmin

Программа предоставляет интерфейс в котором возможно удаленное управление компьютером, режим просмотра и файловый менеджер.

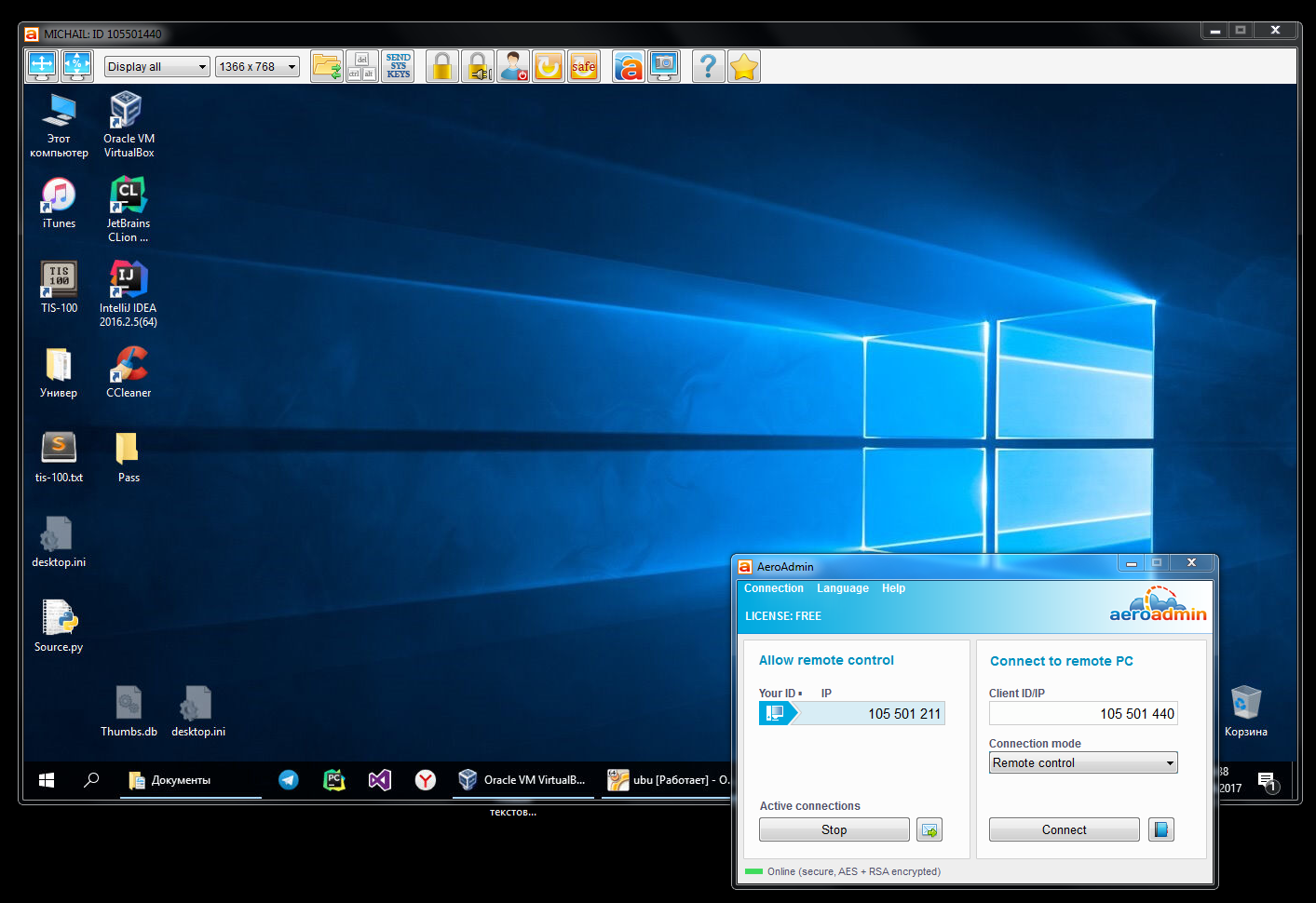


Рис. 2 Удаленное управление компьютером

Удаленный доступ позволяет перехватывать движения мышью, клавиши клавиатуры, работу с файловой системой. Таким образом предоставляется полный доступ к системе.

1. **Протоколы удаленного доступа**

Все программы удаленного доступа реализуют один из известных протоколов, либо же пишут свои протоколы, которые чаще всего являются комерческой тайной.

Здесь мы рассмотрим основные протоколы удаленного доступа и принципы их работы.

* 1. Протокол RDP

RDP (Remote Desktop Protocol — протокол удалённого рабочего стола) — проприетарный протокол прикладного уровня, позаимствованный Microsoft из купленной у PictureTel (ныне известной как Polycom) телекоммуникационной программы Liveshare Plus (названной впоследствии NetMeeting), использующийся для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений. По умолчанию используется порт TCP 3389. Официальное название Майкрософт для клиентского ПО — Remote Desktop Connection или Terminal Services Client (TSC), в частности, клиент в Windows 2k/XP/2003/Vista/2008/7/8/10 называется mstsc.exe.

Особенности версии 5.2, используемой в Windows Server 2003 SP2 и в Windows XP SP3:

Поддержка 32-битного цвета (в дополнение к 8-, 15-, 16-, и 24-битному в предыдущих версиях);

Возможность использовать 128-битовое шифрование по алгоритмам RC4, AES или 3DES с проверкой целостности хешем MD5 или SHA1, по умолчанию не используется, значение безопасности RDP в Windows 2003 по умолчанию — RC2 (56 бит) c хешем MD5 с откатом на DES (40 бит). (Из-за слабого шифрования RC2 и DES при использовании настройки по умолчанию трафик может быть расшифрован по пути, см. тип уязвимости «man-in-the-middle vulnerability»);

Поддержка Transport Layer Security (только при использовании шифрования RC4, AES или 3DES), по умолчанию не включена;

Звук с удалённого ПК переадресовывается и воспроизводится на локальном компьютере;

Позволяет подключать локальные ресурсы к удалённой машине (mapping);

Позволяет использовать локальный или сетевой принтеры на удалённом ПК;

Позволяет приложениям, выполняющимся в пределах текущего сеанса, обращаться к локальным последовательным и параллельным портам;

Можно обмениваться информацией через буфер обмена.

В Windows Vista используется версия 6 протокола RDP, в Windows Server 2008 — версия 6.1, в Windows 7 — версия 7 (по умолчанию, в SP1 можно обновить), в Windows 8 — версия 8.

* 1. Протокол Telnet

Протокол Telnet (TELNET) предназначен для взаимодействия устройств и процессов терминала. TELNET часто применяется программами эмуляции терминала для входа в удаленную систему. TELNET также обеспечивает взаимодействия терминал-терминал и взаимодействия между процессами. Кроме того, TELNET применяется другими протоколами (например, FTP) для создания управляющего канала протокола.

2.3 Протокол пересылки файлов FTP.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Он может использоваться приложениями и пользователями для передачи файлов по сети. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Однако, кроме пересылки файлов, протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Кроме того, FTP позволяет пользователю указывать тип и формат запоминаемых данных. Наконец, FTP выполняет аутентификацию пользователей.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Он может использоваться приложениями и пользователями для передачи файлов по сети. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Однако, кроме пересылки файлов, протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Кроме того, FTP позволяет пользователю указывать тип и формат запоминаемых данных. Наконец, FTP выполняет аутентификацию пользователей. FTP обеспечивает защиту данных при передаче, отправляя внешнему хосту пароль пользователя и учетного файла пользователя.

2.4 Протокол TFTP.

Упрощенный протокол передачи файлов (TFTP) предназначен для обмена файлами с внешними хостами. Для передачи файлов TFTP применяет ненадежный Протокол пользовательских дейтаграмм, поэтому обычно он работает быстрее, чем FTP. Как и FTP, TFTP поддерживает передачу файлов в формате NETASCII и в 8-разрядном двоичном формате. В отличие от FTP, TFTP не поддерживает просмотр каталогов или переход в другой каталог внешнего хоста. В нем также не предусмотрена защита с помощью пароля. Кроме того, TFTP работает только с общими каталогами.

**2.5 Протоколы защищенных каналов SSL, PPTP, IPSec**

Протокол PPTP (Point-to-Point Tunneling Protocol) разработан компанией Microsoft совместно с компаниями Ascend Communications, 3Com/Primary Access, ECI-Telematics и US Robotics. Этот протокол был представлен в рабочую группу "PPP Extentions" IETF в качестве претендента на стандартный протокол создания защищенного канала при доступе удаленных пользователей через публичные сети (в первую очередь Internet) к корпоративным сетям. Этот протокол получил статус проекта стандарта Internet, однако, в качестве стандарта так и не был утвержден. Сейчас рабочая группа IETF рассматривает возможность принятия в качестве стандарта протокол L2TP (Layer 2 Tunneling Protocol), который должен объединить лучшие стороны протокола PPTP с протоколом аналогичного назначения L2F (Layer 2 Forwarding), предложенного компанией Cisco.

Протокол PPTP позволяет создавать защищенные каналы для обмена данными по различным сетевым протоколам — IP, IPX или NetBEUI. Данные этих протоколов инкапсулируются с помощью протокола PPTP в пакеты протокола IP, с помощью которого переносятся в зашифрованном виде через любую сеть TCP/IP. Инкапсулируется исходный кадр РРР, поэтому протокол PPTP можно отнести к классу протоколов инкапсуляции канального уровня в сетевой.

Многопротокольность — основное преимущество инкапсулирующих протоколов канального уровня, к которым относится протокол PPTP. Протокол SSL, например, ориентируется на один протокол сетевого уровня — IP. К тому же размещение протокола защищенного канала непосредственно под прикладным уровнем требует переписи приложений, если они хотят воспользоваться возможностями защиты. Защиты данных на канальном уровне делает средства защиты прозрачными как для протоколов прикладного уровня, так и для протоколов сетевого уровня.

Существуют также и варианты встраивания средств создания защищенного канала на сетевом уровне. Имеется несколько протоколов этого типа, использующих шифрацию и инкапсуляцию протокола сетевого уровня в сетевой. Для защиты данных в IP-сетях разработана защищенная версия протокола IP, которую чаще всего называют IPSec (подробнее о нем поговорим о нем в следующей части статьи). Эта версия поддерживает аутентификацию на сетевом уровне, а также может выполнять шифрацию пользовательских данных. IPSec — это набор стандартов, часть из которых существует в виде проектов, а часть еще находится в стадии разработки. Протокол IPSec не определяет жестко, какие методы шифрации должны использоваться для аутентификации и создания защищенного канала, хотя для первых реализаций определен вариант IPSec, использующий дайджест-функцию MD5 для аутентификации и алгоритм шифрования DES для образования защищенного канала. Недостатком протокола IPSec является то, что он работает только в IP-сетях и не определяет способа защищенной транспортировки пакетов других протоколов. Этот недостаток устраняют такие протоколы, как PPTP или L2F.принцип работы PPTP.

Сетевые протоколы функционируют путем обмена порциями данных, называемыми пакетами. Пакет состоит из управляющей информации, специфичной для протокола, и собственно данных, которые должны быть переданы; их часто называют полезной нагрузкой. До тех пор, пока обмен данными происходит достаточно быстро и без ошибок, нас не волнует, какую управляющую информацию добавляет протокол для своих целей. Но она жизненно важна и должна сохраняться неизменной, если два компьютера собираются обмениваться данными, вне зависимости от среды соединения.  
PPTP работает путем инкапсуляции "родных" пакетов локальной сети — например, пакетов IPX — внутрь пакетов TCP/IP. Весь пакет IPX, включая его управляющую информацию, становится полезной нагрузкой для пакета TCP/IP, который затем можно передавать по Internet. Программные средства на другом конце линии связи извлекают пакет IPX и направляют его для нормальной обработки в соответствии с его собственным протоколом. Этот процесс называется туннелированием, вероятно, потому, что создается коридор в Internet, соединяющий два узла.

Туннелирование позволяет не только экономить на стоимости дальних звонков, но и повышать степень защиты данных. Поскольку туннель соединяет два совместимых протокола с сетью Windows NT/2000, операционная система может выполнять всеобъемлющие проверки надежности защиты, которые она проводит в самой локальной сети. Таким путем соединение может обеспечить принятую в Windows NT/2000 аутентификацию пользователей по протоколам PAP (Password Authentication Protocol) или CHAP (Challenge Handshake Authentication Protocol). Более того, PPTP позволяет передавать данные, зашифрованные RSA-методами RC-4 или DES. Если безопасность подключения к сети VPN является критическим фактором, администратор сервера может указать, что сервер будет принимать посредством дистанционного соединения только пакеты PPTP, но это предотвратит использование сервера в режиме открытого доступа по HTTP или FTP. Однако, если имеется более одного сервера и если нужно обеспечить наивысшую защиту, такое решение — вполне приемлемый вариант.

Но даже при всех подобных мерах безопасности единственным специальным программным обеспечением для клиента служит сам протокол PPTP плюс программа связи по модему, которая может соединить с сетью VPN. И даже это не является необходимым, если у поставщика услуг Internet есть средства работы с PPTP, позволяющие безопасно передавать любые данные по стандартному протоколу PPP (Point-to-Point Protocol, протокол соединения "точка-точка"). процесс связи по протоколу PPTP .

Поскольку вся идея дистанционного доступа состоит в разрешении машине клиента подключаться по телефонной линии к машине сервера, соединение PPTP инициируется клиентом, который использует служебное средство Windows NT — Remote Access Service (RAS) — для установления PPP-соединения с поставщиком услуг Internet. Затем при активизированном соединении PPP с помощью сервера, подключенного к Internet и действующего как сервер RAS, клиент применяет RAS для выполнения второго соединения. На этот раз в поле номера телефона указывается IP-адрес (или доменное имя), и клиент, для того чтобы осуществить соединение, вместо COM-порта использует VPN-порт (VPN-порты конфигурируются на машинах клиента и сервера в процессе инсталляции PPTP).

Ввод IP-адреса инициирует передачу запроса серверу на начало сеанса. Клиент ожидает от сервера подтверждения имени пользователя и пароля и ответа сообщением, что соединение установлено. В этот момент начинает свою работу канал PPTP, и клиент может приступить к туннелированию пакетов серверу. Поскольку они могут быть пакетами IPX и NetBEUI, сервер может выполнять с ними свои обычные процедуры обеспечения защиты.

В основе обмена данными по протоколу PPTP лежит управляющее соединение PPTP — последовательность управляющих сообщений, которые устанавливают и обслуживают туннель. Полное соединение PPTP состоит только из одного соединения TCP/IP, которое требует передачи эхо-команд для поддержания его открытым, пока выполняются транзакции.

**2.4 Усугубление проблем безопасности при удаленном доступе.**

Обеспечение безопасности данных при удаленном доступе - проблема если и не номер один, то, по крайней мере, номер два, после проблемы обеспечения приемлемой для пользователей пропускной способности. А при активном использовании транспорта Internet она становится проблемой номер один.

Неотъемлемым свойством систем удаленного доступа является наличие глобальных связей. По своей природе глобальные связи, простирающиеся на много десятков и тысяч километров, не позволяют воспрепятствовать злонамеренному доступу к передаваемым по этим линиям данным. Нельзя дать никаких гарантий, что в некоторой, недоступной для контроля точке пространства, некто, используя, например, анализатор протокола, не подключится к передающей среде для захвата и последующего декодирования пакетов данных. Такая опасность одинаково присуща всем видам территориальных каналов связи и не связана с тем, используются ли собственные, арендуемые каналы связи или услуги общедоступных территориальных сетей, подобные Internet.

Однако использование общественных сетей (речь в основном идет об Internet) еще более усугубляет ситуацию, хотя бы потому, что в такой сети для доступа к корпоративным данным в распоряжении злоумышленника имеются более разнообразные и удобные средства, чем выход в чистое поле с анализатором протоколов. Кроме того, огромное число пользователей увеличивает вероятность попыток несанкционированного доступа.

Безопасная система - это система, которая, во-первых, надежно хранит информацию и всегда готова предоставить ее своим пользователям, а во-вторых, система, которая защищает эти данные от несанкционированного доступа.

Межсетевой экран (firewall, брандмауэр) - это устройство, как правило, представляющее собой универсальный компьютер с установленным на нем специальным программным обеспечением, который размещается между защищаемой (внутренней) сетью и внешними сетями, потенциальными источниками опасности. Межсетевой экран контролирует все информационные потоки между внутренней и внешними сетями, пропуская данные, в соответствии с заранее установленными правилами. Эти правила являются формализованным выражением политики безопасности, принятой на данном предприятии. Межсетевые экраны базируются на двух основных приемах защиты:

пакетной фильтрации;

сервисах-посредниках (proxy-services).

Эти две функции можно использовать как по отдельности, так и в комбинации.

Пакетная фильтрация. Использование маршрутизаторов в качестве firewall

Фильтрация осуществляется на транспортном уровне: все проходящие через межсетевой экран пакеты или кадры данных анализируются, и те из них, которые имеют в определенных полях заданные ("неразрешенные") значения, отбрасываются.

Пропуск во внутреннюю сеть пакетов сетевого уровня или кадров канального уровня по адресам (MAC-адреса, IP-адреса, IPX-адреса) или номерам портов TCP, соответствующих приложениям. Например, для того, чтобы трафик telnet не пересекал границу внутренней сети, межсетевой экран должен отфильтровывать все пакеты, в заголовке TCP которых указан адрес порта процесса-получателя, равный 23 (этот номер зарезервирован за сервисом telnet). Сложнее отслеживать трафик FTP, который работает с большим диапазоном возможных номеров портов, что требует задания более сложных правил фильтрации.

Конечно, для фильтрации пакетов может быть использован и обычный маршрутизатор, и действительно, в Internet 80% пакетных фильтров работают на базе маршрутизаторов. Однако маршрутизаторы не могут обеспечить ту степень защиты данных, которую гарантируют межсетевые экраны.

Главные преимущества фильтрации межсетевым экраном по сравнению с фильтрацией маршрутизатором состоят в следующем:

межсетевой экран обладает гораздо более развитыми логическими способностями, поэтому он в отличие от маршрутизатора легко может, например, обнаружить обман по IP-адресу;

у межсетевого экрана большие возможности аудита всех событий, связанных с безопасностью.

Сервисы - посредники (Proxy-services) Сервисы-посредники не допускают возможности непосредственной передачи трафика между внутренней и внешней сетями. Для того, чтобы обратиться к удаленному сервису, клиент-пользователь внутренней сети устанавливает логическое соединение с сервисом-посредником, работающим на межсетевом экране. Сервис-посредник устанавливает отдельное соединение с "настоящим" сервисом, работающим на сервере внешней сети, получает от него ответ и передает по назначению клиенту - пользователю защищенной сети.

Для каждого сервиса необходима специальная программа: сервис-посредник. Обычно, защитный экран включает сервисы-посредники для FTP, HTTP, telnet. Многие защитные экраны имеют средства для создания программ-посредников для других сервисов. Некоторые реализации сервисов-посредников требуют наличия на клиенте специального программного обеспечения. Пример: Sock - широко применяемый набор инструментальных средств для создания программ-посредников.

Сервисы-посредники не только пересылают запросы на услуги, например, разработанный CERN сервис-посредник, работающий по протоколу HTTP, может накапливать данные в кэше межсетевого экрана, так что пользователи внутренней сети могут получать данные с гораздо меньшим временем доступа.

Журналы событий, поддерживаемые сервисами-посредниками, могут помочь предупредить вторжение на основании записей о регулярных неудачных попытках. Еще одним важным свойством сервисов-посредников, положительно сказывающимся на безопасности системы, является то, что при отказе межсетевого экрана защищаемый посредником сервис-оригинал остается недоступным.

Трансляция сетевых адресов - новый вид сервиса-посредника. Трансляторы адресов заменяют "внешние" IP-адреса серверов своих сетей на "внутренние". При таком подходе топология внутренней сети скрыта от внешних пользователей, вся сеть может быть представлена для них одним-единственным IP-адресом. Такая непрозрачность сети усложняет задачу несанкционированного доступа. Кроме этого, трансляция адресов дает еще одно преимущество - позволяет иметь внутри сети собственную систему адресации, не согласованную с Internet, что снимает проблему дефицита IP-адресов.

Сервисы-посредники намного надежнее фильтров, однако они снижают производительность обмена данными между внутренней и внешней сетями, они также не обладают той степенью прозрачности для приложений и конечных пользователей, которая характерна для фильтров.

Технология защищенного канала призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например, по сети Internet. Защищенный канал включает в себя выполнение трех основных функций:

взаимная аутентификация абонентов;

защита передаваемых по каналу сообщений от несанкционированного доступа;

подтверждение целостности поступающих по каналу сообщений.

Взаимная аутентификация обеих сторон при установлении соединения может быть выполнена, например, путем обмена сертификатами.

Секретность может быть обеспечена каким-либо методом шифрации, например, передаваемые сообщения шифруются с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрации и дешифрации на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей.

Целостность передаваемых сообщений достигается за счет того, что к сообщению (еще до его шифрации сессионным ключом) добавляется дайджест, полученный в результате применения односторонней функции к тексту сообщения.

Протоколы аутентификации удаленных пользователей.

Контроль доступа пользователей к ресурсам корпоративной сети должен осуществляться в соответствии с политикой безопасности организации, которой принадлежит данная сеть. Эффективное разграничение доступа к сетевым ресурсам может быть обеспечено только при надежной аутентификации пользователей. Требования к надежности аутентификации удаленных пользователей должны быть особенно высокими, так как при взаимодействии с физически удаленными пользователями значительно сложнее обеспечить доступ к сетевым ресурсам. В отличие от локальных пользователей удаленные пользователи не проходят процедуру физического контроля при допуске на территорию организации.

При удаленном взаимодействии важна аутентификация не только пользователей, но и оборудования, поскольку подмена пользователя или маршрутизатора приводит к одним и тем же последствиям — данные из корпоративной сети передаются не тем лицам, которым они предназначены.

Для обеспечения надежной аутентификации удаленных пользователей необходимо выполнение следующих требований:

• проведение аутентификации обеих взаимодействующих сторон — как удаленного пользователя, так и сервера удаленного доступа — для исключения маскировки злоумышленников;

• оперативное согласование используемых протоколов аутентификации;

• осуществление динамической аутентификации взаимодействующих сторон в процессе работы удаленного соединения;

• применение криптозащиты передаваемых секретных паролей либо механизма одноразовых паролей для исключения перехвата и несанкционированного использования аутен-тифицирующей информации.

Протокол РРР имеет встроенные средства, которые могут быть использованы для организации аутентификации при удаленном взаимодействии. В стандарте RFC 1334 определены два протокола аутентификации:

• по паролю — PAP (Password Authentication Protocol);

• по рукопожатию — CHAP (Challenge Handshake Authentication Protocol).

В процессе установления удаленного соединения каждая из взаимодействующих сторон может предложить для применения один из стандартных протоколов аутентификации — РАР или CHAP.

Иногда компании создают собственные протоколы аутентификации удаленного доступа, работающие вместе с протоколом РРР. Эти фирменные протоколы обычно являются модификациями протоколов РАР и CHAP.

Широкое применение для аутентификации по одноразовым паролям получил протокол S/Key. В программных продуктах, обеспечивающих связь по протоколу РРР, протоколы РАР и CHAP, как правило, поддерживаются в первую очередь.

Протокол РАР.

Суть работы протокола РАР довольно проста. В процессе аутентификации участвуют две стороны — проверяемая и проверяющая. Протокол РАР использует для аутентификации передачу проверяемой стороной идентификатора и пароля в виде открытого текста. Если проверяющая сторона обнаруживает совпадение идентификатора и пароля с записью, имеющейся у него в БД легальных пользователей, то процесс аутентификации считается успешно завершенным, после чего проверяемой стороне посылается соответствующее сообщение. В качестве стороны, чья подлинность проверяется, как правило, выступает удаленный пользователь, а в качестве проверяющей стороны — сервер удаленного доступа.

Для инициализации процесса аутентификации на базе протокола РАР сервер удаленного доступа после установления сеанса связи высылает удаленному компьютеру пакет LCP (Link Control Protocol) — протокол управления каналом, указывающий на необходимость применения протокола РАР. Далее осуществляется обмен пакетами РАР. Удаленный компьютер передает по каналу связи проверяющей стороне идентификатор и пароль, введенные удаленным пользователем. Сервер удаленного доступа по полученному идентификатору пользователя выбирает эталонный пароль из БД системы защиты и сравнивает его с полученным паролем. Если они совпадают, то аутентификация считается успешной, что сообщается удаленному пользователю.

Следует особо отметить, что протокол аутентификации РАР, согласно которому идентификаторы и пароли передаются по линии связи в незашифрованном виде, целесообразно применять только совместно с протоколом, ориентированным на аутентификацию по одноразовым паролям, например, совместно с протоколом S/Key. В противном случае пароль, передаваемый по каналу связи, может быть перехвачен злоумышленником и использован повторно в целях маскировки под санкционированного удаленного пользователя.

Протокол S/Key.

Одним из наиболее распространенных протоколов аутентификации на основе одноразовых паролей является стандартизованный в Интернете протокол S/Key (RFC 1760). Этот протокол реализован во многих системах, требующих проверки подлинности удаленных пользователей, в частности в системе TACACS+ компании Cisco.

Перехват одноразового пароля, передаваемого по сети в процессе аутентификации, не предоставляет злоумышленнику возможности повторно использовать этот пароль, так как при следующей проверке подлинности необходимо предъявлять уже другой пароль. Поэтому схема аутентификации на основе одноразовых паролей, в частности S/Key, позволяет передавать по сети одноразовый пароль в открытом виде и, таким образом, компенсирует основной недостаток протокола аутентификации РАР.

Однако следует отметить, что протокол S/Key не исключает необходимость задания секретного пароля для каждого пользователя. Этот секретный пароль используется только для генерации одноразовых паролей. Для того чтобы злоумышленник не смог по перехваченному одноразовому паролю вычислить секретный исходный пароль, генерация одноразовых паролей выполняется с помощью односторонней, т. е. необратимой, функции. В качестве такой односторонней функции в спецификации протокола S/Key определен алгоритм хэширования MD4 (Message Digest Algorithm 4). Некоторые реализации протокола S/Key в качестве односторонней функции используют алгоритм хэширования MD5 (Message Digest Algorithm 5).

Иногда желательно, чтобы пользователь имел возможность сам назначать секретный постоянный пароль. Для осуществления такой возможности спецификация S/Key предусматривает режим вычисления одноразовых паролей не только на основе секретного пароля, но и на основе генерируемого проверяющей стороной случайного числа. Таким образом, в соответствии с протоколом S/Key за каждым пользователем закрепляется идентификатор и секретный постоянный пароль.

Перед тем как проходить аутентификацию, каждый пользователь должен сначала пройти процедуру инициализации очередного списка одноразовых паролей, т. е. фазу парольной инициализации. Данная фаза выполняется по запросу пользователя на сервере удаленного доступа.

Для ускорения процедуры аутентификации определенное число одноразовых паролей, например, несколько десятков, может быть вычислено заранее и храниться на удаленном компьютере в зашифрованном виде.

Протокол аутентификации на основе одноразовых паролей S/Key применяют, в частности, для улучшения характеристик протоколов централизованного контроля доступа к сети удаленных пользователей TACACS и RADIUS.

Централизованный контроль удаленного доступа.

Для управления удаленными соединениями небольшой локальной сети вполне достаточно одного сервера удаленного доступа. Однако если локальная сеть объединяет относительно большие сегменты и число удаленных пользователей существенно возрастает, то одного сервера удаленного доступа недостаточно.

При использовании в одной локальной сети нескольких серверов удаленного доступа требуется централизованный контроль доступа к компьютерным ресурсам.

Рассмотрим, как решается задача контроля доступа к сети удаленных пользователей в соответствии с обычной схемой, когда удаленные пользователи пытаются получить доступ к сетевым ресурсам, которые находятся под управлением нескольких разных ОС. Пользователь дозванивается до своего сервера удаленного доступа, и RAS выполняет для него процедуру аутентификации, например, по протоколу CHAP. Пользователь логически входит в сеть и обращается к нужному серверу, где снова проходит аутентификацию и авторизацию, в результате чего получает или не получает разрешение на выполнение запрошенной операции.

Нетрудно заметить, что такая схема неудобна пользователю, поскольку ему приходится несколько раз выполнять аутентификацию — при входе в сеть на сервере удаленного доступа, а потом еще каждый раз при обращении к каждому ресурсному серверу сети. Пользователь вынужден запоминать несколько разных паролей. Кроме того, он должен знать порядок прохождения разных процедур аутентификации в разных ОС. Возникают также трудности с администрированием такой сети. Администратор должен заводить учетную информацию о каждом пользователе на каждом сервере. Эти разрозненные БД трудно поддерживать в корректном состоянии. При увольнении сотрудника сложно исключить его из всех списков. Возникают проблемы при назначении паролей, существенно затрудняется аудит.

Отмеченные трудности преодолеваются при установке в сети централизованной службы аутентификации и авторизации. Для централизованного контроля доступа выделяется отдельный сервер, называемый сервером аутентификации. Этот сервер служит для проверки подлинности удаленных пользователей, определения их полномочий, а также фиксации и накопления регистрационной информации, связанной с удаленным доступом. Надежность защиты повышается, если сервер удаленного доступа запрашивает необходимую для аутентификации информацию непосредственно у сервера, на котором хранится общая БД системы защиты компьютерной сети.

Однако в большинстве случаев серверы удаленного доступа нуждаются в посреднике для взаимодействия с центральной БД системы защиты, например, со службой каталогов.

Большинство сетевых ОС и служб каталогов сохраняют эталонные пароли пользователей с использованием одностороннего хэширования, что не позволяет серверам удаленного доступа, стандартно реализующим протоколы РАР и CHAP, извлечь открытый эталонный пароль для проверки ответа.

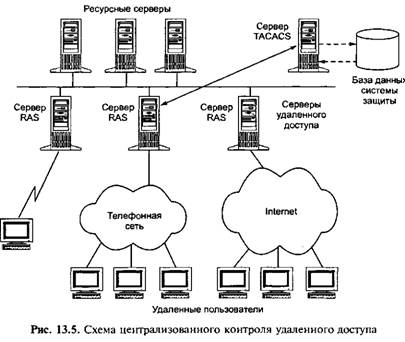
Роль посредника во взаимодействии между серверами удаленного доступа и центральной БД системы защиты может быть возложена на сервер аутентификации. Централизованный контроль удаленного доступа к компьютерным ресурсам с помощью сервера аутентификации выполняется на основе специализированных протоколов. Эти протоколы позволяют объединять используемые серверы удаленного доступа и сервер аутентификации в одну подсистему, выполняющую все функции контроля удаленных соединений на основе взаимодействия с центральной БД системы защиты. Сервер аутентификации создает единую точку наблюдения и проверки всех удаленных пользователей и контролирует доступ к компьютерным ресурсам в соответствии с установленными правилами.

К наиболее популярным протоколам централизованного контроля доступа к сети удаленных пользователей относятся протоколы TACACS (Terminal Access Controller Access Control System) и RADIUS (Remote Authentication Dial-In User Service). Они предназначены в первую очередь для организаций, в центральной сети которых используется несколько серверов удаленного доступа. В этих системах администратор может управлять БД идентификаторов и паролей пользователей, предоставлять им привилегии доступа и вести учет обращений к системным ресурсам.

Протоколы TACACS и RADIUS требуют применения отдельного сервера аутентификации, который для проверки подлинности пользователей и определения их полномочий может использовать не только собственную БД, но и взаимодействовать с современными службами каталогов, например, с NDS (Novell Directory Services) и Microsoft Windows NT Directory Service.

Серверы TACACS и RADIUS выступают в качестве посредников между серверами удаленного доступа, принимающими звонки от пользователей, с одной стороны, и сетевыми ресурсными серверами — с другой. Реализации TACACS и RADIUS могут также служить посредниками для внешних систем аутентификации.

Рассмотрим особенности централизованного контроля удаленного доступа на примере протокола TACACS.

[](http://ypn.ru/wp-content/uploads/2010/09/13.5.jpg)

Система TACACS выполнена в архитектуре клиент-сервер. В компьютерной сети, включающей несколько серверов удаленного доступа, устанавливается один сервер аутентификации, который называют сервером TACACS (обычно это программа, работающая в среде универсальной ОС, чаще всего Unix).

На сервере TACACS формируется центральная база учетной информации об удаленных пользователях, включающая их имена, пароли и полномочия. В полномочиях каждого пользователя задаются подсети, компьютеры и сервисы, с которыми он может

работать, а также различные виды ограничений, например, временные ограничения. На этом сервере ведется БД аудита, в которой накапливается регистрационная информация о каждом логическом входе, продолжительности сессии, а также времени использования ресурсов сети.

Клиентами сервера TACACS являются серверы удаленного доступа, принимающие запросы на доступ к ресурсам сети от удаленных пользователей. В каждый такой сервер встроено ПО, реализующее стандартный протокол, по которому они взаимодействуют с сервером TACACS. Этот протокол также называется TACACS.

**4 Практическая часть**

В качестве практической части было предложено написать программу, моделирующую процесс перехвата пакетов в виртуальной сети. Программа была написана на языке Python 2.7 в программной среде PyCharm 2017.1.1. Полный код программы представлен в приложении 1, но мы рассмотрим её основные фрагменты.

**4.1 Построение плоского изображения дерева**

Исходный граф, по которому строится дерево, задается матрицей смежности. Изображение дерева в программе имеет вид упорядоченного списка вершин – объектов класса *TVertex*. В объекте класса содержится информация о номере вершины, её уровне в дереве, ссылка на вершину-предка (null, если это корень дерева) и список ссылок на дочерние вершины (у висячих вершин этот список будет пуст). Вершина *v* имеет позицию *i* в списке дерева, если *v* стоит на

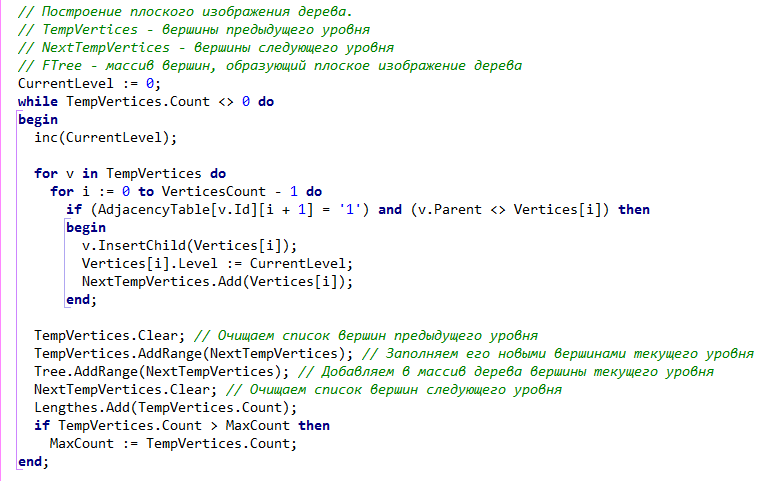


Рисунок 8

уровне *k* дерева и , где – число вершин на *j*-ом уровне дерева, – порядковый номер вершины *v* на *k*-ом уровне. Код построения этого списка представлен на рисунке 8. Этот список вместе со служебной информацией представлен классом *TTree*.

**4.2 Построение кода Прюфера**

Код Прюфера в программе представляет из себя простой массив из *n* – 2 элементов, состоящий из элементов множества *M*. Помимо самого кода для визуализации также потребовалось поддерживать упорядоченный список удалённых рёбер в порядке их удаления из графа. Алгоритм принимает на вход матрицу смежности графа, на выходе – код Прюфера и упорядоченный список удалённых рёбер. Код алгоритм представлен на рисунке 9.

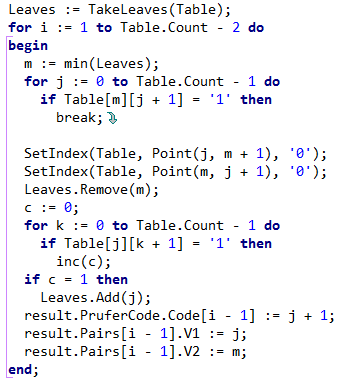


Рисунок 9

Таким образом программа повторяет алгоритм, описанный в главе 2. Запускаем цикл *n* – 2 раз, на каждом его шаге программа находит минимальный лист, ребро, связанное с этим листом, удаляет это ребро из графа, удаляет висячую вершину из списка всех висящих (список *Leaves*) и добавляет, если необходимо, смежную с удалённой вершину (добавление происходит, если эта вершина стала висячей). При этом в ответ добавляется номер этой смежной вершины.

**4.3 Построение плоского изображения дерева из кода Прюфера**

Алгоритм построения плоского изображения дерева из кода Прюфера принимает на вход последовательность Прюфера, а на выход отдает упорядоченный список вершин, как в главе 3.1 – объект класса *TTree*. Программа повторяет алгоритм, описанный в главе 2. Фрагмент кода представлен на рисунке 10.

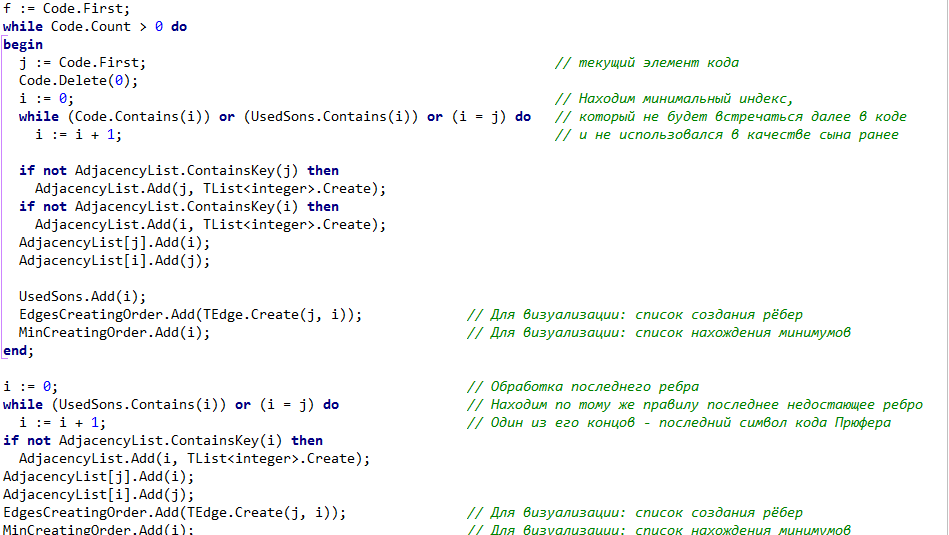


Рисунок 10

Основной цикл выполняется пока в коде Прюфера ещё есть номера вершин. На каждом шаге: вынимаем первый номер из последовательности – *j*, удаляем первый (только что вытащенный) элемент из последовательности. Затем ищем минимальный номер вершины, не встречающийся в коде и не использованный ранее (массив *UsedSons*) – переменная *i*. Добавляем в граф ребро (*i*, *j*), обновляем служебные списки. Граф для удобства будет представлен списком смежности – *AdjacencyList* – список списков. *i*-ый список содержит номера вершин, смежных с вершиной *i*.

**ЗАКЛЮЧЕНИЕ**

Построение плоского изображения дерева является достаточно простой задачей, в то время как построение кода Прюфера и построение дерева по коду Прюфера являются достаточно серьезными задачами. Однако самое применение кода Прюфера для кодирования графа даёт большой выигрыш в объёме, занимаемым деревом в памяти компьютера. С другой же стороны, код Прюфера не позволяется анализировать исходное дерево, модифицировать и вообще каким-либо способом изменять его в конкретных целях.

В заключение можно сказать, что код Прюфера является эффективным контейнером, хранящим в себе исходное дерево. Помимо этого, алгоритм конструирования кода Прюфера даёт точную оценку количества неориентированных деревьев, состоящих из *n* вершин, а именно .

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Богомолов, А.М. Алгебраические основы теории дискретных систем [Текст] / А.М. Богомолов, В.Н. Салий –Москва: «Физико-математическая литература» РАН, 1997. –367с.

2. Березина, Л.Ю. Графы и их применение [Текст] / Березина Л.Ю. –Москва «Просвещение», 1979. –142с.

**ПРИЛОЖЕНИЕ 1**