УДК 004.771

УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ

Бондаренко Р. С.[1], студент гр.153504, Тушинская Е.В.[2],магистрант гр.256241

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Рогов М.Г. – ассистент кафедры информатики

Аннотация. Исследование сфокусировано на проблематике удаленного администрирования компьютерных систем и сетей. Особое внимание уделяется анализу существующих технологий и методов обеспечения безопасности при удаленной администрации. В работе также исследуется вопрос настройки удаленного доступа через интернет и локальные сети, включая решения для работы с динамическими IP-адресами. Цель исследования - выявить современные тренды и проблемы в области удаленного администрирования, а также предложить рекомендации по повышению эффективности и безопасности данного процесса.

Ключевые слова. Удаленное администрирование, установочные средства, нежелательное по, согласие пользователя, нежелательные галочки, методы обмана, осведомленность пользователей, установочные параметры, безопасность it, программное обеспечение, архитектуры удаленного доступа, протоколы удаленного управления, динамические ip-адреса, технологии удаленного доступа, эффективное удаленное управление.

Понятие «системы удаленного управления» охватывает разнообразные аспекты, включая архитектуры, протоколы, программы и скрипты, определяющие эффективную работу таких систем. Это не только включает в себя обнаружение ошибок и реагирование на них, но и управление повседневными задачами, такими как установка программного обеспечения или добавление новых пользователей. Для централизованного и эффективного контроля всех аспектов компьютерной системы требуются надежные технологии удаленного доступа .

На сегодняшний день существует множество программ, которые обеспечивают удаленный доступ к компьютеру через интернет или локальную сеть. Обычно такие программы состоят из двух модулей: клиентского и серверного. Клиентский модуль устанавливается на том компьютере, с которого осуществляется удаленное управление, а серверный - на удаленном компьютере или компьютерах.

Когда удаленный компьютер доступен напрямую через интернет и имеет статический IP-адрес, настройка обычно довольно проста. Однако, если доступ осуществляется через маршрутизатор или прокси-сервер, который имеет доступ в интернет, может потребоваться настройка перенаправления портов или использование специальных утилит для установки виртуального соединения между компьютерами.

Если у удаленного компьютера динамический IP-адрес, возникают дополнительные сложности, поскольку IP-адрес изменяется при каждом подключении. В таких случаях часто используются услуги подобные DynDNS, которые отслеживают изменения IP-адреса и предоставляют постоянное DNS-имя для доступа к компьютеру.

На рынке существует множество приложений, многие из которых ориентированы на корпоративный сектор. Эти приложения обычно предлагают широкий спектр функциональности, включая удаленное управление компьютерами, мониторинг состояния системы, диагностику проблем, а также возможности автоматизации задач.

Некоторые программы предоставляют различные варианты лицензирования, которые подходят как для корпоративных клиентов, так и для домашних пользователей. Это может включать опции подписки, пакетные предложения для компаний различного размера, а также бесплатные версии для некоммерческого использования.

Важно учитывать такие факторы, как надежность, безопасность, производительность, а также соответствие специфическим потребностям организации или пользователя. Некоторые из популярных приложений в этой области включают TeamViewer, AnyDesk, Remote Desktop Manager, Kickidler, и другие. Каждое из этих приложений имеет свои особенности и преимущества, поэтому выбор зависит от конкретных потребностей и предпочтений пользователя.

TeamViewer – широко используемое решение для удаленного управления и организации конференций через интернет или локальную сеть. Эта программа позволяет получить доступ к рабочему столу

удаленного компьютера с возможностью полного управления им. Также она позволяет записывать сеансы удаленного управления для последующего просмотра и обмениваться файлами с поддержкой функции перетаскивания [2].

Это одно из самых известных и широко используемых приложений для удаленного администрирования компьютеров и проведения онлайн-презентаций. Мощное и удобное в использовании приложение, которое позволяет пользователям получать доступ к удаленным компьютерам или устройствам с любого места, где есть интернет-соединение.

Одним из ключевых преимуществ TeamViewer является его простота установки и использования. Пользователи могут легко настроить удаленное соединение без необходимости в сложной конфигурации или специальных навыков. Благодаря этому TeamViewer подходит как для профессиональных администраторов IT, так и для обычных домашних пользователей.

Возможность передачи файлов между компьютерами, проведение онлайн-презентаций, а также использование дополнительных инструментов для обеспечения безопасности и конфиденциальности данных – это важные особенности.

TeamViewer также предлагает различные варианты лицензирования, включая бесплатные версии для некоммерческого использования, а также платные планы с расширенными функциями для корпоративных клиентов. Это делает приложение доступным для широкого круга пользователей и позволяет выбрать оптимальный вариант в соответствии с конкретными потребностями и бюджетом.

Программа TeamViewer представлена в виде одного инсталляционного модуля, который устанавливается как на компьютере, с которого планируется осуществлять контроль, так и на удаленном ПК. Пример представлен на рисунке 1.1.

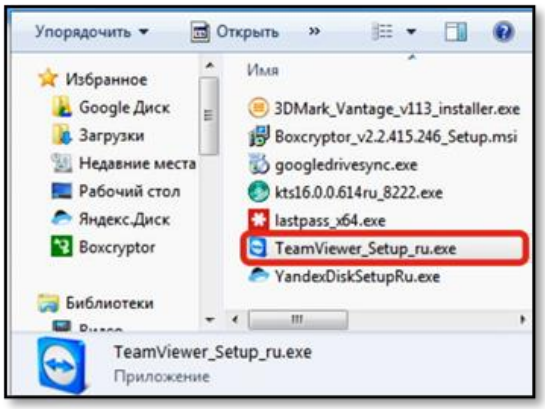

Рисунок 1.1 – Инсталляционного модуля

После открытия файла «TeamViewer_Setup_ru.exe», откроется окно в котором нужно нажать кнопку «Запустить». Пример представлен на рисунке 1.2.

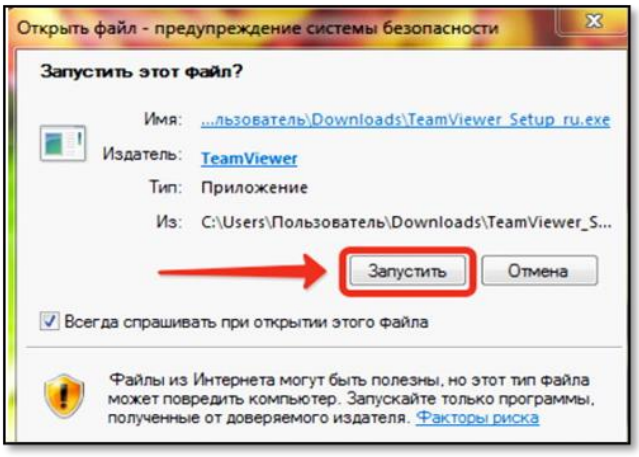

Рисунок 1.2 – Всплывающее окно при установке TeamViewer

Далее нужно выбрать между пунктами «Установить», «Установить, чтобы потом управлять этим компьютером удаленно» и «Только запустить». А также выбрать схему использования, которая подходит под поставленные задачи. В качестве примера были выбраны пункты «Установить» и «Личное/некоммерческое использование». После этих манипуляций нужно нажать кнопку «Принять». Все представлено на рисунке 1.3.

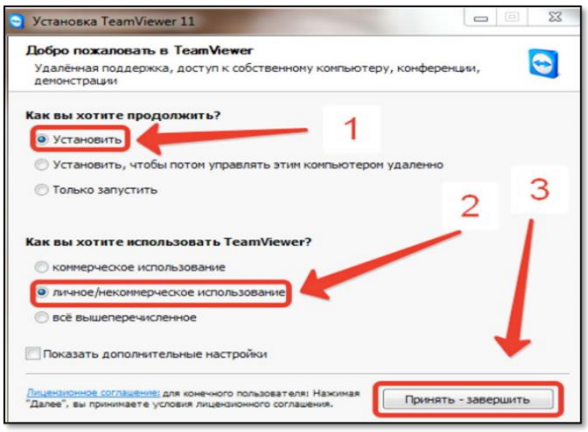

Рисунок 1.3 – Установка TeamViewer

Разработчики предоставили возможность использовать TeamViewer для создания частной виртуальной сети (VPN), организации конференций и демонстраций. Приложение поддерживает голосовое и видеообщение между компьютерами, а также работает через брандмауэры, NAT-маршрутизаторы и прокси без необходимости дополнительной настройки. Оно автоматически оптимизирует качество отображения и скорость передачи данных в зависимости от типа подключения к сети (LAN, мобильное устройство и т. д.). С точки зрения безопасности, соединения устанавливаются через полностью зашифрованные каналы, используя обмен 1024-битными RSA-ключами и шифрование сеанса AES с длиной ключа 256 бит. Алгоритм представлен на рисунке 1.4.

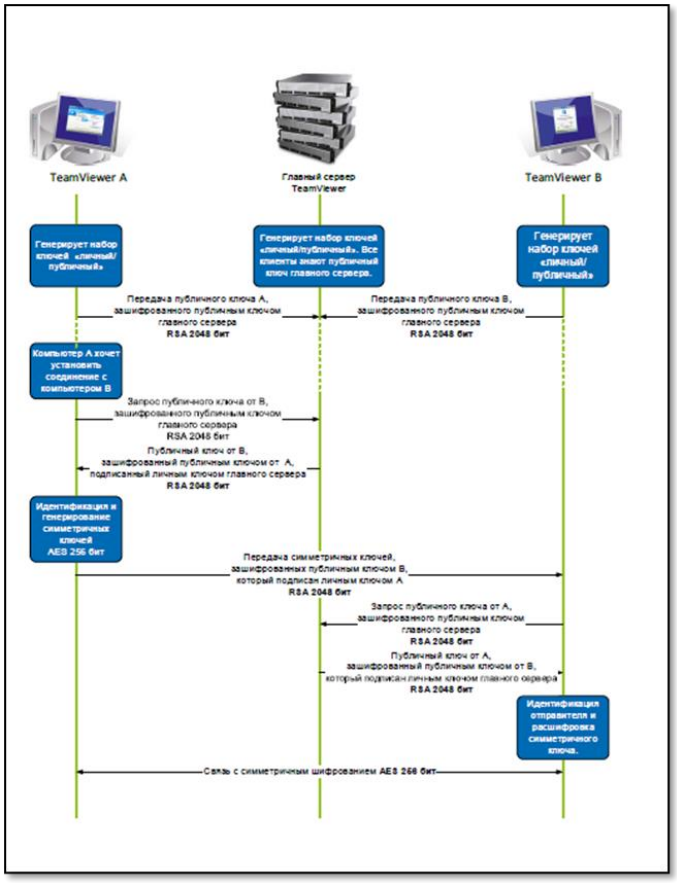

Рисунок 1.4 – Схема соединения в TeamViewer

RSA (Rivest-Shamir-Adleman) – это криптографический алгоритм, который используется для шифрования и дешифрования данных, а также для подписи и проверки цифровых подписей. Он основан на использовании двух ключей: публичного и приватного [3].

Публичный и приватный ключи связаны математически таким образом, что данные, зашифрованные с использованием публичного ключа, могут быть дешифрованы только с помощью соответствующего приватного ключа, и наоборот. Это обеспечивает возможность безопасного обмена информацией между участниками процесса, не раскрывая приватного ключа.

Внутреннее строение алгоритма RSA основано на математической задаче факторизации больших простых чисел. Процесс генерации ключей начинается с выбора двух различных простых чисел, которые используются для вычисления значения модуля (n). Затем находится значение функции Эйлера от числа n, обозначаемой как φ(n). Далее выбирается открытый экспонент (обычно это простое число, такое как 65537), который обычно выбирается для оптимизации производительности алгоритма шифрования.

Публичный ключ состоит из открытого экспонента и значения модуля (e, n), а приватный ключ содержит секретный экспонент (d), который вычисляется на основе открытого экспонента и значения функции Эйлера.

Шифрование данных с использованием публичного ключа позволяет зашифровать сообщение таким образом, что его может расшифровать только обладатель соответствующего приватного ключа. Для этого используется операция возведения в степень по модулю n. Дешифрование происходит путем возведения зашифрованного сообщения в степень по модулю n с использованием секретного экспонента. Пример RSA ключа представлен на рисунке 1.5.

Рисунок 1.5 – RSA ключ

RSA является одним из самых широко используемых алгоритмов шифрования в мире, благодаря своей безопасности и надежности. Однако, для эффективного использования алгоритма RSA важно выбирать достаточно большие простые числа для обеспечения надежной защиты данных.

AES (Advanced Encryption Standard) – это симметричный алгоритм шифрования, применяемый для защиты конфиденциальности данных. Он был разработан как замена устаревшим стандартам шифрования, таким как DES (Data Encryption Standard), и сегодня является одним из самых распространенных и надежных алгоритмов шифрования в мире [4].

Внутреннее строение алгоритма AES основано на процессе подстановки и перестановки битов, известном как Substitution-Permutation Network. Он состоит из четырех основных операций: AddRoundKey, SubBytes, ShiftRows и MixColumns, которые последовательно выполняются на каждом раунде шифрования.

Операция AddRoundKey осуществляет побитовое сложение (XOR) каждого байта состояния с соответствующим байтом ключа раунда. SubBytes заменяет каждый байт состояния на соответствующий байт из таблицы замены (S-Box), придавая шифру дополнительную нелинейность.

ShiftRows циклически сдвигает каждую строку состояния на определенное количество байт влево, а MixColumns выполняет линейные преобразования над столбцами состояния, что увеличивает его сложность и стойкость к криптоанализу.

AES поддерживает три варианта длины ключа: AES-128, AES-192 и AES-256, соответствующие ключам длиной 128, 192 и 256 бит соответственно. Более длинные ключи обеспечивают высокий уровень безопасности, но требуют больше вычислительных ресурсов для шифрования и дешифрования данных. Пример AES шифрования представлен на рисунке 1.6.

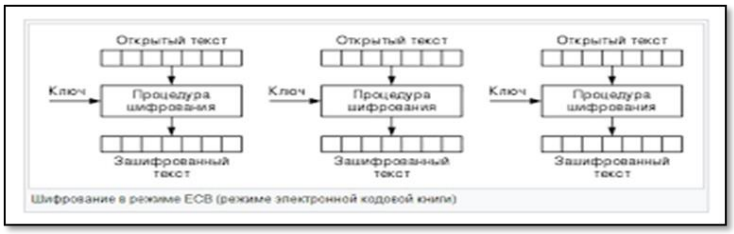

Рисунок 1.6. AES шифрование

Для мгновенного запуска на удаленном компьютере можно использовать компактный модуль TeamViewer QuickSupport, который скачивается отдельно и не требует установки или прав администратора. Также существует «портативная» версия для мобильного использования, которую можно запустить с USB-накопителя или CD. Настройка удаленного доступа с помощью.

TeamViewer предоставляет простой способ подключения к удаленному компьютеру: при установке программы ему автоматически присваиваются уникальный ID и пароль. При желании подключиться к удаленному компьютеру, достаточно указать эти данные на ПК администратора.

Такой подход позволяет избежать необходимости работать с IP-адресами, перенаправлением портов и другими техническими аспектами. В то же время, можно настроить подключение через IP-адрес в локальной сети, но это потребует корректировки настроек программы. Кроме того, вход в систему удаленного компьютера можно осуществить, используя учетные данные Windows, такие как имя пользователя и пароль., представлено на рисунке 1.7.

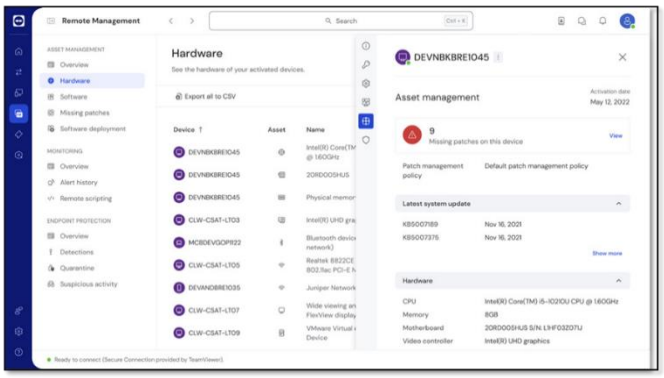

Рисунок 1.7 – TeamViewer

Этот программный продукт мультиплатформенный, работает на macOS, Linux, Windows и Android. Благодаря облачным сервисам управления, можно использовать TeamViewer в браузерах без установки на компьютер.

TeamViewer позволяет не только управлять удаленными компьютерами, но и оборудованием, подключенным к ним, включая принтеры и курсоры. Кроме того, возможна передача файлов и обмен текстовыми, аудио- и видеосообщениями в режиме реального времени, что облегчает общение и сотрудничество.

Плюсы TeamViewer включают бесплатную загрузку и установку, доступ к облачным сервисам и возможность перетаскивания файлов между удаленным и локальным рабочим столом.

Однако существуют и некоторые недостатки. TeamViewer имеет ограничение на размер передаваемых файлов, что может привести к снижению производительности при обмене большими файлами. Кроме того, программа не работает через прокси-серверы, что может быть неудобно для некоторых пользователей. При низкой скорости интернет-соединения некоторые функции TeamViewer могут замедляться, включая управление курсором и передачу файлов.

Список использованных источников:

1. "Службы удаленного рабочего стола" [Электронный ресурс]. Режим доступа: https://docs.microsoft.com/ru-ru/windows-server/remote/remote-desktop-services/welcome-to-rds/. Дата доступа: 27.04.2024.

2. "TeamViewer - программное обеспечение для удаленного рабочего стола" [Электронный ресурс]. Режим доступа: https://www.teamviewer.com/. Дата доступа: 28.04.2024.

3. "Удаленный доступ к компьютеру" [Электронный ресурс]. Режим доступа: https://www.remotedesktop.com/. Дата доступа: 01.05.2024.

UDC 004.771

REMOTE ADMINISTRATION

Bondarenko R.S. [1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Rogov M.G. – Assistant of the Department of Informatics

Annotation. The research is focused on the problems of remote administration of computer systems and networks. Particular attention is paid to the analysis of existing technologies and methods for ensuring security during remote administration. The work also examines the issue of setting up remote access via the Internet and local networks, including solutions for working with dynamic IP addresses. The purpose of the study is to identify current trends and problems in the field of remote administration, as well as offer recommendations for increasing the efficiency and security of this process

Keywords. Remote administration, installation tools, junkware, user consent, unwanted checkmarks, deception techniques, user awareness, settings, it security, software, remote access architectures, remote management protocols, dynamic IP addresses, remote access technologies, effective remote management .