

## Описание системы безопасности Radmin 3

### Система безопасности Radmin

Программы удаленного администрирования предоставляют широкий спектр возможностей как для компаний, так и для домашних пользователей. Однако, всякий раз, открывая доступ к своему компьютеру, пользователь рискует тем, что доступ к нему может получить злоумышленник. Следовательно, решения удаленного доступа должны обеспечивать максимальную безопасность, чтобы доступ к компьютерам могли получить именно те люди, для которых этот доступ предназначен.



Долгое время на компьютерных форумах, посвященных вопросам безопасности, защита Radmin 2.2 называлась “параноидальной”. Такое название она заслужила после того, как в 2004 году компанией “Фаматек” была проведена специальная акция: на компьютер с выходом в интернет был установлен сервер Radmin 2.1, и тот, кому удалось бы взломать защиту и получить доступ к компьютеру мог получить денежный приз. За шесть с лишним месяцев работы сервера взломать его не удалось никому.

Новая версия Radmin 3 предлагает пользователям улучшенную систему безопасности, и включает в себя широкий набор решений для обеспечения максимально безопасного доступа к удаленным компьютерам. Новая система безопасности предоставляет следующие возможности:

#### **1. Пользователь может выбирать между использованием собственной системы безопасности Radmin или системы безопасности Windows**

Система безопасности была существенно улучшена по сравнению с предыдущей версией программы. Собственная система аутентификации Radmin теперь поддерживает имена пользователей с набором прав для них. Новый метод аутентификации использует улучшенный алгоритм Диффи-Хеллмана с 2048-битным ключом. Случайный ключ для каждого соединения и проверка целостности данных позволяют защитить процесс аутентификации от любых попыток несанкционированного доступа, включая одну из самых опасных — использование “злоумышленника-посредника”.

Radmin также поддерживает систему аутентификации Windows, таким образом давая возможность администраторам домена использовать привычные средства задания прав пользователям и группам.

## 2. Radmin не сохраняет пароли доступа и не передает их по сети

В отличие от конкурентов, Radmin обеспечивает секретность паролей даже если кто-либо получает физический доступ к локальному или удаленному компьютеру. Серверная часть программы сохраняет не пароль, а его контрольную сумму (hash), которую и использует для аутентификации. При этом даже если кто-либо получает доступ к контрольной сумме пароля на сервере, эту контрольную сумму невозможно использовать для аутентификации не зная текстового пароля.

Клиентская часть программы не позволяет сохранять вводимые пароли, так что даже если кто-либо получит доступ к клиентскому компьютеру у него не будет возможности воспользоваться удаленным доступом не зная пароля, что имеет особое значение для крупных компаний с большим количеством рабочих мест. При подключении клиентской части программы к серверной пароль также не передается ни в какой форме. И наконец, пароль доступа нельзя получить анализируя сетевой трафик программы.

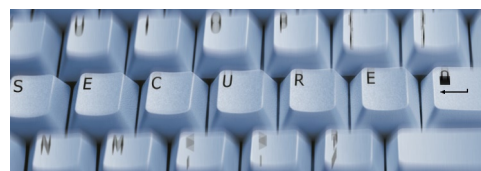


## 3. Надежная защита всех передаваемых данных

При использовании как собственной системы аутентификации Radmin так и системы аутентификации Windows, все передаваемые по сети данные (нажатия клавиш, изменения экрана, передаваемые файлы и т. д.) надежно защищены. При этом для каждого соединения используется случайный ключ и все полученные данные проверяются на целостность, что позволяет предотвращать несанкционированное изменение данных. В отличие от конкурентов, Radmin использует защиту данных не как “дополнительную возможность”, а как одно из основных средств обеспечения безопасности. Защиту данных нельзя отключить, она интегрирована в ядро программы. Оптимизированный код программы и продуманные протоколы обмена данными позволяют осуществлять защиту данных почти без потери производительности, используя менее 5% ресурсов процессора.

## 4. Защита от попыток подобрать пароль к работающему серверу

Radmin обеспечивает безопасность даже если пользователи используют очень простые пароли доступа. Серверная часть программы автоматически определяет попытки подбора пароля и использует интеллектуальную систему задержек и блокировок для их предотвращения.



## 5. IP фильтрация

Для обеспечения максимальной безопасности серверная часть программы может быть настроена таким образом, чтобы разрешать соединения только с указанных IP адресов. Даже если пароль пользователя станет известен злоумышленнику, этот пароль нельзя будет использовать для подключения извне.



## 6. Запрос на подтверждение соединения

Серверная часть Radmin может быть настроена таким образом, чтобы запрашивать подтверждение пользователя на подключение к компьютеру. Это позволяет предотвратить случайные подключения к удаленному компьютеру без разрешения пользователя.

## 7. Защита настроек сервера

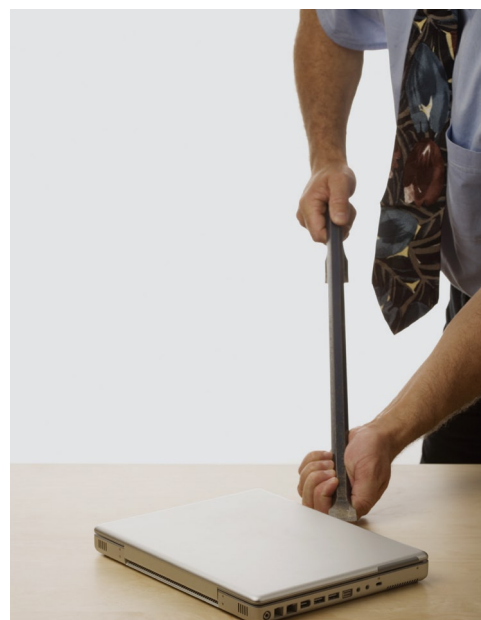
Настройки серверной части Radmin защищены от неавторизованного изменения. Они не могут быть изменены пользователями, не имеющими прав администратора на удаленном компьютере.

## 8. Запрет на использование пустых паролей

Подключение к серверу Radmin возможно только при условии использования одной из двух систем аутентификации: Radmin или Windows. При этом запрещено задавать пустой пароль.

## 9. Исполняемые файлы программы защищены от модификаций и имеют цифровую подпись

Код исполняемых модулей Radmin содержит надежную защиту от модификаций и проверку на целостность. Если кто-либо попытается встроить в Radmin код для перехвата вводимых паролей, то программа просто не запустится, сообщив о том что ее код был модифицирован. Программа также защищена от изучения (reverse engineering) как в виде исполняемого файла, так и в виде запущенного приложения. Исполняемые файлы программы содержат цифровую подпись компании "Фаматек" для подтверждений их аутентичности.



## 10. Протокол соединений

Серверная часть Radmin ведет протокол соединений в виде HTML-файла. Эта информация может быть использована для аудита подключений к удаленному компьютеру и для выявления потенциально опасного поведения, например, попыток подобрать пароль или соединений в нерабочее время. Кроме того, Radmin поддерживает ведение протокола событий Windows.

## От каких угроз защищает система безопасности Radmin

Почему так важно защитить удаленные компьютеры от неавторизованного доступа? Очевидная причина – это защита ваших частных данных, паролей, номеров кредитных карт и другой важной информации, которая может находиться на удаленном компьютере. Но есть и другие причины, которые важно учитывать при выборе программного обеспечения для организации удаленного доступа:



- В крупных компаниях пользователи часто используют простые пароли и записывают их в общедоступных местах. Radmin эффективно блокирует попытки подбора пароля, не позволяя сохранять пароль и не допуская настроек серверной части без защиты паролем.
- Пользователи могут загрузить из сети или получить по электронной почте небезопасные программы, которые, не являясь вирусами, тем не менее снижают настройки безопасности системы. Radmin не зависит от настроек безопасности системы и защищает от модификации собственные исполняемые файлы.
- В локальных сетях, особенно беспроводных, всегда есть опасность перехвата сетевого трафика и попыток получить неавторизованный доступ к внутренним сетевым ресурсам путем его анализа и модификаций. Radmin защищает всю передаваемую по сети информацию и не передает пароли доступа ни в каком виде. Сервер Radmin надежно защищен от попыток неавторизованного доступа путем анализа, замены или модификации сетевого трафика.
- Возможность доступа к удаленным компьютерам может быть заблокирована из-за DOS атак, нарушения работы или стабильности серверных программ. Серверная часть Radmin эффективно предотвращает DOS атаки и рассчитана на круглосуточную бесперебойную работу в течении долгого времени. Сервер Radmin всегда использует минимальное количество системных ресурсов и обладает высокой стабильностью и надежностью работы.