А. А. Алтухов[1,2,3]

[1]Россия, Москва, ЗАО «ОКБ САПР»
[2]Московский физико-технический институт (государственный университет)
[3]Национальный исследовательский ядерный университет «МИФИ»

ДОВЕРЕННЫЙ СЕАНС СВЯЗИ НА СЛУЖБЕ АКАДЕМИЧЕСКОГО ПРОЦЕССА

Рассматривается способ работы по предоставлению студентам вуза безопасного удаленного доступа к информационно-техническим ресурсам в рамках академического процесса, для научно-исследовательской деятельности, а также удаленной работы в рамках стажировки.

В настоящее время обычным явлением становится возможность выполнять свои рабочие обязанности, находясь за пределами периметра компаний. Удаленный доступ к инфраструктуре, необходимой для выполнения своих рабочих или учебных обязанностей, является одним из признаков общества постиндустриального, общества информационного. Данный способ работы позволяет оптимизировать некоторые возможные издержки и максимизировать эффективность и вместе с тем прибыль. Возможность работать из любой точки мира позволяет не выпадать из рабочего процесса во время поездок и позволяет экономить время на перемещение из дома до офиса. Современные технологии типа SaaS, PaaS, IaaS наряду с активно развивающимися облачными технологиями являются эффективным и экономичным решением многих задач.

Обеспечение отказоустойчивости, надежности и безопасности корпоративных информационных систем является одной из важных задач. Эта задача может и сложная, но стандартная. Проблемы начинают возникать, когда подключение к информационной системе осуществляется извне физического периметра. С подобной проблемой автор столкнулся на кафедре «Защиты информации» Московского Физико-Технического Института Государственного Университет, базовое предприятие – ЗАО «ОКБ САПР».

В рамках академического процесса для освоения различных дисциплин по специальности, проведения лабораторных работ и ведения научно-исследовательской деятельности кафедра предоставляет материально-техническое обеспечение (аппаратное и программное), также обеспечивается возможность проходить стажировку на предприятии и получать реальный опыт работы в отрасли. Из соображений эффективности и экономии материально-техническое обеспечение создается на основе инфраструктуры базового предприятия. Реализация удаленного доступа в настоящий момент не является проблемой. Существует много различных технологий, в частности VPN. Именно эту технологию мы использовали для решения нашей задачи. Реальная проблема оказалась в том, как обеспе-

чить безопасный доступ. В первую очередь компанию интересует именно безопасность инфраструктуры, к которой студент будет получать доступ. При проектировании решения данной проблемы рассмотрены следующие возможные риски инфраструктуры: утеря студентом учетных данных для удаленного подключения; возможность осуществлять несанкционированные действия в инфраструктуре, как самим студентом, так и похитителем учетных данных; безопасный удаленный доступ к необходимым ресурсам. Для минимизации рисков, связанных с вышеприведенными угрозами, меры принимаются в разных частях информационной системы, в том числе и на стороне, предоставляющей ресурсы.

В данной работе рассматриваются лишь те меры, которые были приняты на клиентской стороне взаимодействия. При обеспечении безопасного клиент-серверного доступа необходимо учитывать безопасность сервера, канала связи и клиента.

Обеспечение безопасности сервера (поставщика сервисов) не является чем-то необычным. С защитой канала тоже проблем нет. Существует много различных технологий, которые позволяют организовать защищенный доступ к удаленным информационным ресурсам. С клиентами дело обстоит несколько иначе. Серьезные проблемы возникают, когда клиентские устройства осуществляют подключения к информационной системе извне периметра. Здесь возникает важный и существенный вопрос, каким образом можно обеспечить безопасность клиента.

Концептуальное решение данной задачи уже давно известно, и один из стандартных способов организации защищенного доступа пользователей к удаленной информационной системе обеспечивается применением VPN в доверенной среде. На удаленном рабочем месте должна быть обеспечена доверенная среда для организации защищенного доступа. Организация подключения к удаленным ресурсам должна осуществляться только из доверенной среды. Только в этом случае мы можем гарантировать как безопасность подключения, так и невозможность получения учетных данных удаленного доступа студента злоумышленником, например, с помощью трояна. В составе доверенной среды должен быть только определенный набор функций, который может быть использован удаленным пользователем при доступе к ресурсам. Естественно необходимо минимизировать затраты на данное решение.

Одним из возможных способов решения – это предоставление студенту средства вычислительной техники (СВТ) с настроенной доверенной средой, реализованной функцией доверенной загрузки и необходимым минимальным набором программного обеспечения. Подобным средством может быть ноутбук. Однако это достаточно дорогое решение и для многих студентов связанно с различными ограничениями. Особенно проблемы возникают, если они не могут использовать данное решение для выполнения личных задач. В такой среде они не будут полноправными владельцами и администраторами системы. Данное решение обычно подходит тем, у кого нет своего персонального средства вычислительной техники. Также в данном подходе следует отметить наличие лишних издержек, связанных с задачей администрирования данной единицы техники.

В большинстве случаев у современных студентов есть своя ЭВМ, с которой они хотели бы получать доступ. На данном СВТ скорее всего нет доверенной среды. Более того, у базового предприятия нет возможности убедиться, что данная среда будет организована в момент предоставления доступа.

Следует отметить, что уже существует решение задачи организации доверенного сеанса связи (ДСС), которое используются как для решения задач клиент-банкинга и взаимодействия с государственными услугами, так и для безопасного удаленного доступа. Для рассматриваемого в докладе вопроса парадигма ДСС применима, так как нам необходимо обеспечить доверенную вычислительную среду на определенный короткий срок для задачи доступа к удаленным ресурсам.

На базе аппаратной платформы устройства «МАРШ!» было спроектировано устройство, призванное решить поставленную проблему. Устройство состоит из аппаратной и программной части. Аппаратная часть обеспечивает управление доступом к памяти. С точки зрения управления доступом устройство на базе платформы «МАРШ!» представляет собой память, разделенную на несколько разделов.

На проектируемом устройстве один раздел доступен только для чтения (ReadOnly), на данном разделе расположена операционная система и необходимый минимальный набор программного обеспечения для доступа к удаленным ресурсам и выполнения поставленной учебной задачи. Два раздела скрыты для пользователя и доступны лишь для программных компонент доверенной среды. Один из них доступен только для чтения (ReadOnly), в нем хранится необходимая ключевая информация и учетные данные для удаленного доступа. Обратим внимание, что пользователь не обладает данной информацией и не может использовать ее в другой среде. Второй из них, ПО доверенной среды, может переводить в состояние «только на добавление» (AddOnly). Этот раздел используется резидентным софтом из доверенной среды для ведения журналов событий.

В состав резидентного программного обеспечения входит операционная система, VPN, программное обеспечение для удаленного доступа. В резидентной операционной системе настроено разграничение доступа. Пользователь не обладает правами администратора ОС и имеет возможность выполнять только тот функционал, который необходим для решения поставленных задач и определяется базовым предприятием (владельцем удаленной информационной системы). Перед входом в ОС происходит аутентификация пользователя по паролю, который передается пользователю вместе с устройством. Следует отметить, что способы аутентификации могут быть различны, но в конкретной реализации был выбран именно такой способ.

Данное устройство студент может использовать для создания доверенной среды в те моменты времени, когда ему необходимо поработать с предоставляемыми кафедрой ресурсами. Для загрузки доверенной среды он вполне может использовать свой персональный компьютер, общественный компьютер в институте или компьютер своего соседа по комнате.

При этом базовое предприятие получает гарантии, что подключение к удаленным ресурсам будет происходить только из доверенной среды. Потеря учетных данных удаленного доступа возможна только вместе с устройством.

В случае утери для доступа к резидентной операционной системе необходима аутентифицирующая информация. На случай получения данной информации злоумышленником средства в доверенной среде ограничены в функциональности и не позволяют злоумышленнику получить широкий комплекс возможностей воздействия на удаленную систему.

Таким образом, базовое предприятие может минимизировать свои риски, связанные с предоставлением ресурсов для студентов.