КОНТРОЛЬ ДЕЙСТВИЙ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ, ПОДКЛЮЧАЕМЫХ ПО ТЕХНОЛОГИЯМ УДАЛЕННОГО РАБОЧЕГО СТОЛА И ВИРТУАЛЬНЫХ РАБОЧИХ СТОЛОВ WINDOWS

Проскурняк Сергей Михайлович

студент, Тольяттинский государственный университет, РФ, г. Тольятти

Хрипунов Николай Владимирович

научный руководитель, Тольяттинский государственный университет, РФ, г. Тольятти

Аннотация. В статье рассмотрен способ контроля действий удаленных пользователей, подключаемых по технологиям удаленного рабочего стола и виртуальных рабочих столов Windows. В качестве технологии защиты предложено использовать драйвер-фильтр файловой системы ОС Windows. Разработаны контекстная диаграмма проектируемого программного продукта, его диаграмма использования, включающая 2 фактора, и диаграмма классов проектируемого программного обеспечения, включающая 3 класса.

Ключевые слова: информационная безопасность, информационное обеспечение, удаленный доступ, контроль удаленного доступа, драйвер-фильтр.

В настоящее время технологии удаленного доступа к информационным системам (ИС) широко распространены, и доля их использования продолжает возрастать. Это связано как с экономическими и социальными преимуществами (отсутствует необходимость содержания рабочего помещения, доставки работников до места работы, более свободный режим работы), так и с решением проблем, определяемых современными вызовами (например, пандемией вируса COVID19). В то же время технологии удаленного доступа потенциально уязвимы для различного рода угроз, связанных с возможностью сетевых атак и недобросовестностью удаленных пользователей. В этой связи предпринимаются различные меры защиты удаленного подключения, общим стандартом которых стало использование виртуальных частных сетей (VPN).

Использование VPN в значительной мере решает проблему защиты от внешнего нарушителя, но не может защитить от действий недобросовестных удаленных пользователей. Это определяет необходимость контроля действий пользователей при их удаленном подключении. Решению этой проблемы посвящена данная работа.

В настоящее время развитие технологий удаленного доступа привело к разработке следующих способов его осуществления [1]:

1) подключение к персональному техническому средству, включенному в ЛВС организации;

2) инфраструктура виртуальных рабочих столов [2];

3) виртуализация приложений [2].

При использовании наиболее легкого в реализации первого способа осуществляется

подключение пользователя к некоторому определенному компьютеру сети организации. Практические реализации данного метода осуществляется встроенными службами ОС Windows Server: службой удаленного рабочего стола и служба терминального доступа. Эти два вида доступа иногда отождествляются [3], в других источниках отмечается их различия, в частности, «отличия между компонентами Удаленный рабочий стол (Remote Desktop) и Службы терминалов (Terminal Services) заключаются в том, что Службы терминалов предоставляют больше возможностей для расширяемости, а также содержат много дополнительных важных компонентов. Например, на компьютере Windows Server 2008 с включенным компонентом Удаленный рабочий стол (Remote Desktop) лишь два пользователя могут одновременно подключиться к активному сеансу рабочего стола (в том числе все локальные пользователи активных консольных сеансов). Таких ограничений не существует на сервере с установленными и отконфигурированными службами терминалов» [4].

Второй способ организации удаленного доступа, реализующий инфраструктуру виртуальных рабочих столов (Virtual Desktop Infrastructure, VDI), позволяет создавать виртуальную IT-инфраструктуру и организовывать рабочие места на базе одного или нескольких серверов в виде виртуальных машин [5]. При этом удаленный пользователь подключается к специальному серверу, на котором запускается виртуальная машина, с которой и происходит работа [2]. Наиболее популярные практические реализации этой технологии:

1.«Инфраструктура виртуальных рабочих столов (VDI) – решение, позволяющее запустить ОС пользователя (Windows 7 и т.д.) внутри виртуальной машины на сервере в ЦОД и работать с ней удаленно с любого устройства (Citrix XenDesktop, VMware View, Microsoft VDI, Quest vWorkspace)»[6].

2.«Службы удаленных рабочих столов или терминальные сервисы (Remote Desktop Services Host (RDSH) / Terminal Services (TS)) – классический терминальный доступ, предоставляющий серверную операционную систему (обычно, Windows Server) нескольким пользователям в конкурентном режиме. Каждый из удаленных пользователей работает в своей сессии. Наиболее популярные решения – Citrix XenApp, Microsoft RDS, Quest vWorkspace»[6].

3.«Удаленная физическая рабочая станция (Blade PC) – мощная высокопроизводительная рабочая станция (часто с установленным графическим адаптером) в форм-факторе сервера, расположенная в ЦОД, и предоставляющая свои вычислительные ресурсы удаленным пользователям. Наиболее популярные решения – Citrix HDX 3D Pro + Dell R5500, VMware View + Dell R5500»[6].

Третий способ удаленного доступа – виртуализация приложений – «позволяет использовать приложения, установленные на сервере, так, как будто бы они установлены на рабочем компьютере сотрудника» [5]. Пример такой платформы – «Microsoft Application Virtualization (App-V), разработанная компанией Microsoft» [6], а также «Citrix XenApp, VMware ThinApp» [3].

Во всех случаях удаленного подключения непосредственное подключение к сети Интернет имеют не все устройства, к которым происходит удаленное подключение, и используется отдельный сервер доступа, на котором устанавливается специальное программное обеспечение, осуществляющее аутентификацию клиента и передачу сетевых пакетов от удаленного клиента к серверу или объекту управления и обратно.

Рассмотренные технологии удаленного доступа слишком разнообразны, чтобы осуществить контроль предоставляемого с их помощью удаленного доступа каким-то одним программным продуктом. В этой связи необходимо рассмотреть вопрос о выборе той технологии, которую разрабатываемое программное средство будет контролировать.

При этом необходимо отметить, что технологии виртуализации приложений предполагают удаленный запуск определенного приложения (например, в финансовых учреждениях это автоматизированная банковская система, АБС), специально предназначенного для осуществления работы оператора, так что его доступ и, соответственно, контроль доступа целиком ложится на это приложение. Поэтому контроль такого типа удаленного доступа нами рассматриваться не будет.

Технологии удаленного рабочего стола и виртуальных рабочих столов, напротив, могут предоставлять пользователям реальный доступ к информационным ресурсам, и контроль этого доступа необходимо организовать. Учитывая, что подавляющее большинство настольных компьютеров и ноутбуков в России работают под управлением ОС семейства Windows (в том числе и в организациях финансовой сферы), именно на контроль удаленного доступа к рабочим столам таких операционных систем необходимо обратить внимание в первую очередь. Это и будет направлением, которому будет посвящена данная работа.

С точки зрения работы операционной системы удаленный пользователь, подключаемый по технологии удаленного рабочего стола или виртуальных рабочих столов, не отличим от пользователя, непосредственно залогиневшегося в систему. Для контроля его доступа ОС Windows применяет методы аудита безопасности.

Однако эти методы могут оказаться неэффективными при наличии у пользователя администраторских прав. Локальный администратор может отключить аудит конкретных объектов ФС, а также удалить данные аудита. Поэтому есть смысл разработать альтернативную методику контроля доступа.

Эта методика может быть реализована на основе технологии перехвата файловых операций пользователя, что в ОС семейства Windows может быть осуществлено при помощи установки драйвера-фильтра файловой системы [7]. Аналогичная технология используется при работе систем антивирусной защиты.

Устанавливаемый в систему драйвер-фильтр может сохранять действия пользователя в специальный файл, передавать данные о них по сети администратору безопасности или для анализа системы обнаружения атак, осуществлять теневое копирование (зеркалирование) файлов, к которым происходит обращение, и др.

Альтернативной технологией контроля доступа при удаленной работе может стать механизм трассировки событий для Windows (ETW) [8]. Он позволяет программистам запускать и останавливать сеансы трассировки событий, создавать приложения для предоставления событий трассировки и использования событий трассировки в приложениях режима пользователя. Такими событиями могут быть события доступа к объектам файловой системы, и обработка этих событий может выполняться аналогично описанному выше.

Преимуществом этого подхода является относительная простота разработки и отладки приложений в режиме пользователя в сравнении с драйверами, работающими в режиме ядра. В свою очередь, драйвер-фильтр более надежен в том смысле, что его, во-первых, сложнее обнаружить, и во-вторых, сложнее выгрузить.

Поэтому в качестве используемой технологии выберем первую, основанную на модели драйвера-фильтра.

На рисунке 1 показана контекстная диаграмма проектируемого программного обеспечения системы контроля доступа удаленного пользователя. Удаленный пользователь осуществляет обращения к файловой системе ИС. Администратор безопасности выполняет настройку системы и получает из нее отчеты о доступе удаленного пользователя.

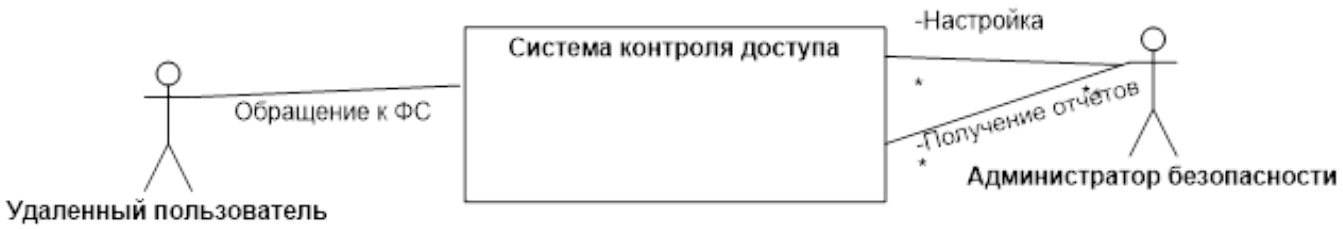

Рисунок 1. Контекстная диаграмма проектируемого программного обеспечения

На рисунке 2 приведена концептуальную модель проектируемой программной системы (диаграмма вариантов использования).

Диаграмма содержит два фактора – удаленного пользователя и администратора безопасности. Показаны варианты обращений удаленного пользователя к файловой системе (чтение, изменение, создание, удаление, выполнение, смена атрибутов), возможные варианты аудита действий удаленного пользователя (логирование и зеркалирование), а также действия администратора безопасности (настройка системы и получение из нее отчетов о действиях удаленного пользователя).

Рисунок 2. Диаграмма вариантов использования проектируемого программного обеспечения

Программное средство планируется построить по клиент-серверной технологии. При этом серверная часть должна совмещать деятельность драйвера-фильтра и взаимодействовать (получать настройки или предоставлять данные) клиентской части по сети.

На рисунке 3 приведена возможная диаграмма классов проектируемого программного продукта.

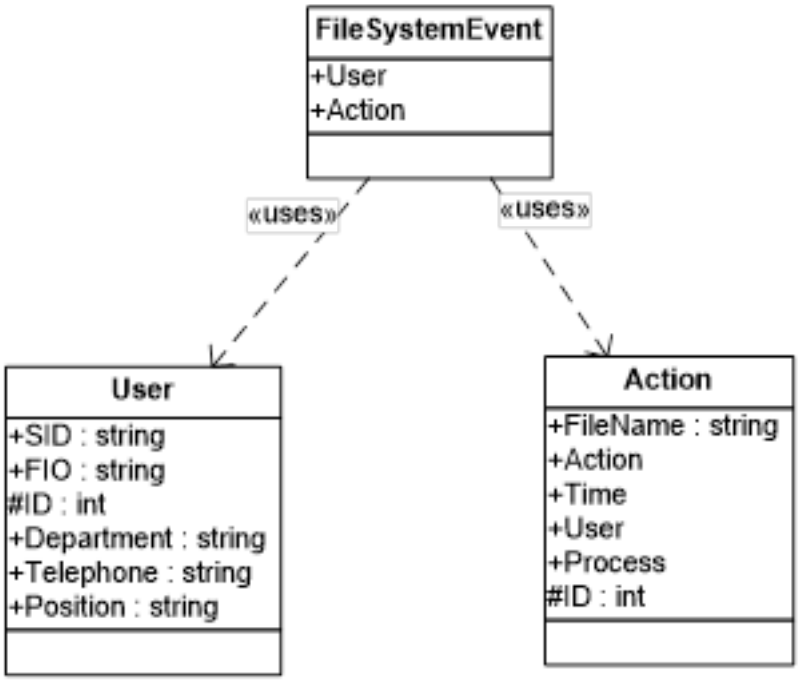

Рисунок 2.2. Диаграмма классов проектируемого программного обеспечения

В ней введено три класса.

Класс User описывает сущность удаленного пользователя. Назначение полей:

– SID – идентификатор безопасности пользователя;

– FIO – фамилия, имя, отчество пользователя;

– ID – внутренний номер пользователя;

– Department – подразделение пользователя;

– Telephone – телефон для экстренной связи;

– Position – должность.

Класс Action описывает сущность действия над объектом файловой системы. Назначение полей:

– FileName – полное имя файла;

– Action – тип события (чтение, создание, удаление и т.д.);

– Time – дата и время события;

– Process – полное имя файла процесса, выполнившего событие в контексте пользователя;

– ID – внутренний номер пользователя.

Класс FileSystemEvent описывает сущность событие файловой системы. Назначение полей:

– User – пользователь, в чьем контексте совершено событие;

– Action – действие над объектом файловой системы.

Для разработки драйверов рекомендуется использование языка программирования C++. Разработка может быть выполнена в Microsoft Visual Studio версии не ниже 2017. Поэтому в качестве средства разработки целесообразно выбрать последнюю на текущий момент версию – Microsoft Visual Studio 2022.

Таким образом, выполненное изучение современных технологий удаленного доступа, современных технологий защиты удаленного доступа позволили выбрать защищаемую технологию удаленного доступа, технологию контроля удаленного доступа, а также выполнить проектирование структуры и компонентов программного продукта и произвести выбор основных средств реализации программного продукта.

Список литературы:

1. Довгаль В. А., Меретукова С. К., Шередько Д. И. Организация безопасного удаленного доступа сотрудника коммерческой компании, работающего вне офиса. // Вестник Адыгейского государственного университета. – Серия 4: Естественно-математические и технические науки. – 2021. – №2 (281). URL: https://cyberleninka.ru/article/n/organizatsiya-bezopasnogo-udalennogo-dostupa-sotrudnika-kommercheskoy-kompanii-rabotayuschego-vne-ofisa (дата обращения: 01.02.2023).

2. Савельев А. Remote Desktop виртуализация // Национальный Открытый Университет «ИНТУИТ». URL: https://intuit.ru/studies/courses/2324/624/lecture/13610 (дата обращения: 01.02.2023).

3. Службы удаленных рабочих столов. // Wikipedia. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.7a726f7e-63d271ab-f709941e-74722d776562/https/en.wikipedia.org/wiki/Microsoft_Terminal_Server (дата обращения: 26.01.2023)

4. Кауфман Е. А. Анализ существующих видов терминального доступа и инфраструктуры VDI // Актуальные вопросы экономических наук. – 2013. – №34. URL: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-vidov-terminalnogo-dostupa-i-infrastruktury-vdi (дата обращения: 26.01.2023).

5. Глоссарий // Документация TIONIX. URL: https://docs.tionix.ru/2.8.17/glossary/index.html#term-vdi-virtual-desktop-infrastructure (дата обращения: 01.02.2023).

6. VMware View-Virtual Desktop Infrastructure - VDI // Российский Интернет-портал и аналитическое агентство "Tadviser". URL: https://www.tadviser.ru/index.php/Продукт:VMware_View_-_Virtual_Desktop_Infrastructure_-_VDI?cache=no&ptype=integr (дата обращения: 01.02.2023).

7. Йосифович П. Работа с ядром Windows. – СПб.: Питер, 2021. – 400 с: ил. — (Серия «Для профессионалов»).

8. Трассировка событий. // Microsoft. – 22.09.2022. URL: https://learn.microsoft.com/ru-ru/windows/win32/etw/event-tracing-portal (дата обращения: 09.02.2023).