ISSN 2306-1561
Automation and Control in Technical Systems (ACTS)
2014, No 4, pp. 149-157.
DOI: 10.12731/2306-1561-2014-4-15

Research Problem of the Virus Security for Computer Network Department of «Automated Control Systems» MADI

Zbavitel Pavel Yuryevich

Russian Federation, Undergraduate Student, Department of «Automated Control Systems».

State Technical University – MADI, 125319, Russian Federation, Moscow, Leningradsky prospekt, 64. Tel.: +7 (499) 151-64-12. http://www.madi.ru

zbavitelpavel@gmail.com

Nikolaev Andrey Borisovich

Russian Federation, Honoris Causa, Doctor of Technical Sciences, Professor, Dean of the Faculty «Control Systems».

State Technical University – MADI, 125319, Russian Federation, Moscow, Leningradsky prospekt, 64. Tel.: +7 (499) 151-64-12. http://www.madi.ru

nikolaev.madi@mail.ru

Abstract. This article discusses options for protecting network computers from viruses. A review of possible solutions. Compares the features of anti-virus software, Deepfreeze program, cloud storage and FTP-server. The advantages and disadvantages of each solution. Shows an embodiment of FTP-server.

Keywords: computer virus security, computer aid software, Deepfreeze, cloud storage, computer network, FTP-server.

ISSN 2306-1561
Автоматизация и управление в технических системах (АУТС)
2014. – №4. – С. 149-157.
DOI: 10.12731/2306-1561-2014-4-15

УДК 004.9

Исследование подходов к решению проблемы вирусоустойчивости сети кафедры “Автоматизированные системы управления” МАДИ

Збавитель Павел Юрьевич

Российская Федерация, магистрант кафедры «Автоматизированные системы управления».

ФГБОУ ВПО «Московский автомобильно-дорожный государственный технический университет (МАДИ)», 125319, Российская Федерация, г. Москва, Ленинградский проспект, д.64, Тел.: +7 (499) 151-64-12, http://www.madi.ru

zbavitelpavel@gmail.com

Николаев Андрей Борисович

Российская Федерация, Лауреат премии правительства РФ, Заслуженный деятель науки РФ, доктор технических наук, профессор, декан факультета «Управление».

ФГБОУ ВПО «Московский автомобильно-дорожный государственный технический университет (МАДИ)», 125319, Российская Федерация, г. Москва, Ленинградский проспект, д.64, Тел.: +7 (499) 151-64-12, http://www.madi.ru

nikolaev.madi@mail.ru

Аннотация. В статье рассматриваются варианты защиты компьютеров сети кафедры Автоматизированные системы управления (АСУ) Московского автомобильно-дорожного государственного технического университета (МАДИ) от вирусов. Дан обзор возможных решений. Представлено сравнение возможностей антивирусного программного обеспечения (ПО), программы Deepfreeze, облачных хранилищ и FTP-сервера. Описаны преимущества и недостатки каждого решения. Показан вариант реализации FTP-сервера, как оптимальное, малозатратное и эффективное решение проблемы вирусоустойчивости сети кафедры.

Ключевые слова: вирусоустойчивость, антивирусное ПО, Deepfreeze, облачное хранилище, компьютерная сеть, FTP-сервер.

1. Введение

Возможность защищенной передачи информации является актуальной темой в настоящее время. Каждый день создается более 10 тысяч компьютерных вирусов. Выбор средств защиты является одной из приоритетных задач.

Одной из главных проблем организации с большим количеством компьютеров, к которым в том числе относится и кафедры АСУ МАДИ, является обеспечение политики безопасности рабочих станций и компьютерной сети, в частности вирусоустойчивости. Заражение стационарных компьютеров вредоносным ПО происходит по большей части через съемные носители информации, такие как: USB-флеш диски, жесткие диски, мобильные устройства и т.д. [1, 7]

В большинстве случаев заражение компьютеров вредоносным ПО происходит посредством использования внешних носителей информации. Следовательно, защиту ПК можно разделить на два условных типа:

- усиление защиты и вирусоустойчивости ПК – подразумевает использование стороннего программного обеспечения, такого как антивирусы или программ оперирующих Snapshot’ми т.е. позволяющих «заморозить» информацию во время работы, а после перезагрузки восстановить к исходному состоянию. Примером таких программ является Deep Freeze.
- отказ от съемных носителей. При этом необходимо обеспечить использование альтернативного способа передачи информации.

Ниже проведен анализ возможных подходов к решению проблемы вирусоустойчивости сети, и далее предложено, по мнению авторов, инновационное решение, основанное на применении FTP-сервера.

2. Анализ возможных подходов к решению проблемы вирусоустойчивости сети

В настоящий момент остро стоит проблема антивирусной защиты сети кафедры АСУ МАДИ. Наиболее активно ранее использовалась защита с помощью антивирусных программ установленных на каждом персональном компьютере. Однако из-за загруженности рабочей станции большим количеством программ для организации учебной деятельности, использование антивируса на ПК стало сильно влиять на работоспособность каждого из них. Также необходимо сказать о постоянном вмешательстве системного администратора в учебный процесс для решения данной проблемы (обновление антивируса, восстановление ПК после системного сбоя и т.п.) Закупка нового более мощного оборудования - процесс длительный и экономически затратный в рамках ВУЗа. В результате выше изложенного было принято решение об отказе использования USB-дисков и внешних носителей информации. Существует несколько возможных решений организации вирусоустойчивости сети кафедры ВУЗа. (антивирусное ПО, программа Deepfreeze, облачные хранилища, FTP-сервер).

2.1. Антивирусное программное обеспечение

Антивирусная программа производит блокировку и удаление вирусов, червей и троянских программ, также препятствует их распространению. Защищает от вредоносного ПО и препятствует возможному заражению [6 – 10]. Защита Anti-Rootkit - предотвращает захват управления компьютером посторонними лицами. Антивирусная защита постоянно совершенствуется для всех пользователей. Анализирует файлы до их загрузки и обеспечивает защиту файлов при использовании служб мгновенного обмена сообщениями.

Преимущества – антивирус обеспечивает многоуровневую защиту рабочих станций и серверов, обладает централизованным управлением. Установка и обновление на компьютерах производится из консоли сервера. Защита распространяется на съемные носители.

Антивирусное ПО создает повышенную нагрузку на рабочие станции, не гарантирует целостность зараженных файлов, что явно относится к недостаткам использования. Также современные антивирусы полностью не обеспечивают очистку компьютера от вредоносных программ и алгоритмов. Современная стратегия борьбы с компьютерными вирусами очень схожа с иммунной системой живых организмов. Сначала у какой-либо компьютер должен заразиться и заболеть, после этого образец вируса должен быть отправлен на сервер производителя антивируса, специалисты разработчика антивирусного ПО проработают, проанализируют вирус, поместят его в базу данных, и только после этого пользователю будет дана возможность лечения зараженных программ и файлов.

2.2. Программное решение с помощью утилиты Deep Freeze

Deep Freeze – утилита для операционных систем которая позволяет защитить ядро операционной системы, а также конфигурационные файлы на рабочей станции или сервере от нежелательных изменений и восстановить первоначальные настройки системы каждый раз после перезагрузки компьютера, независимо от того, случайно это сделано или злонамеренно [5].

Программа является драйвером, работающим на уровне ядра, который защищает работоспособность и целостность жёсткого диска путём направления текущей информации на целый диск или его раздел, в результате исходные данные остаются без изменений. После подобных перенаправлений информации запись на них не ссылается и, после перезагрузки компьютера система восстанавливается в исходное состояние в сектор диска. Такие методы позволяют пользователям создавать «виртуальные» изменения в системе, изменять основные файлы или даже удалять их, делая систему неработоспособной, не боясь экспериментировать, потому что после обычной перезагрузки системы все настройки, которые были «заморожены» восстановятся.

Достоинства утилиты в том, что она сохраняет исходную конфигурацию рабочей станции. Возможность вмешательства в работу программы имеется только у системного администратора. Имеется широкий спектр настроек, например, можно создать

расписание, по которому будет автоматически отключаться «заморозка» на время обновления ПО на компьютере.

Отрицательным моментом использования Deep Freeze является отсутствие возможности защитить операционную систему и жёсткий диск, на котором он установлен, если компьютер загружается из другой среды, например, с внешнего жёсткого диска, USB-устройства, оптического носителя или сетевого сервера. В таких случаях злоумышленник будет иметь возможность доступа к якобы «замороженным» файлам. Можно добавить, что использование данного ПО полностью не решит проблему вирусоустойчивости, так как использование съемных носителей останется необходимым, более того, Deep Freeze не может «заморозить» и восстановить файлы на съемных носителях. Затраты на использование программы Deep Freeze составляет около 45$ в год на одну рабочую станцию. Также ПО создает повышенную нагрузку на жёсткие диски и процессоры рабочих станций, во время запуска и завершения работы операционной системы. Требуется установка на каждый компьютер отдельно.

2.3. Облачные технологии

Последующие решения подразумевают ограничение использования пользователями внешних носителей информации с помощью контроллера домена и групповых политик.

Альтернативным методом решения проблемы является использование готовых решений на базе облачных хранилищ, таких как Google Drive, Яндекс диск и т.д. Эти сервисы за время своей работы зарекомендовали себя на очень высоком уровне.

Достоинствами облачных технологий являются: низкая вероятность утери информации, высокая отказоустойчивость, наличие возможности настройки прав доступа к файлам, отсутствие необходимости заниматься приобретением, поддержкой и обслуживанием собственной инфраструктуры по хранению данных, что, в конечном счёте, уменьшает общие затраты. Также все процедуры по резервированию и сохранению целостности данных производятся провайдером облачного центра.

К недостаткам облачных технологий можно отнести, в первую очередь, недостаточную организованность хранения одних и тех же файлов для большого количества людей (например, задания для лабораторных работ). Преподавателю придется передавать задание каждому студенту в отдельности. К тому же, всем студентам будет необходимо зарегистрироваться на одном и том же, заранее выбранном, хранилище, что само по себе достаточно сложно организовать. Объем хранилища будет достаточен для каждого студента в отдельности, но для хранения данных всей группой необходимо будет заводить несколько хранилищ, использовать множество аккаунтов, что в свою очередь усложнит поиск информации. Более того в процесс передачи информации между домашним компьютером и кафедральным будет включен лишний узел, тем самым добавив сложности (рисунок 1).

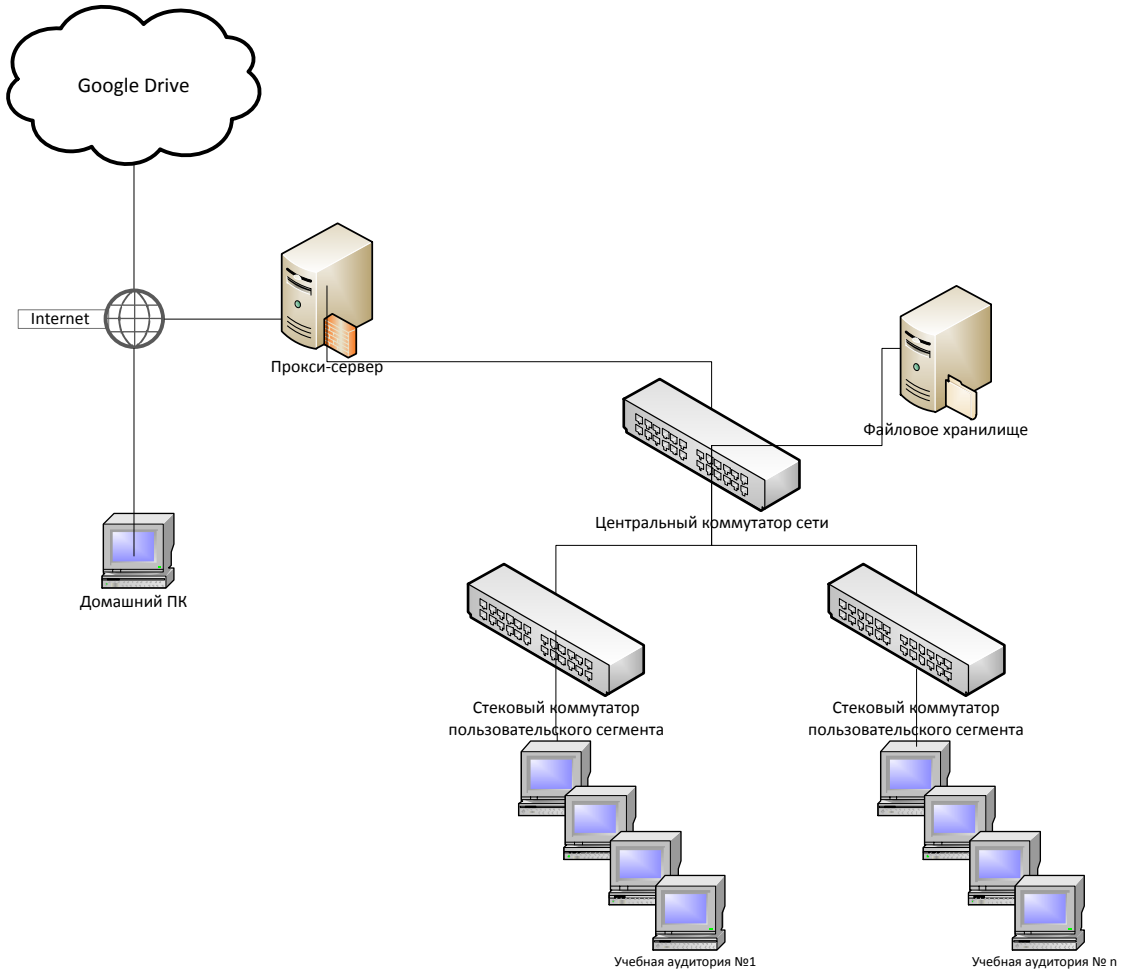

Рисунок 1 – Схема передачи данных с использованием облачного хранилища

3. Подход к решению проблемы вирусоустойчивости сети, основанный на применении FTP-сервера

Все выше изложенные методы имеют ряд недостатков, исходя из которых можно сделать вывод о том, что рационально использовать альтернативный подход, основанный на применении FTP-сервера.

Для решения поставленной задачи на кафедре АСУ МАДИ был создан FTP-сервер для передачи информации, с установленным на него антивирусным программным обеспечением.

Для организации FTP-сервера необходимо:

- Сервер, который должен удовлетворять следующим требованиям (минимальные характеристики):
  - процессор 64-разрядный 1,4 ГГц;
  - оперативная память 512 МБ;
  - место на диске 32 ГБ;
  - операционная система Windows 2008 r2 или выше.
- Локальная сеть с доступом в интернет и пропускной способностью минимум 100 МБ/с.

– Файловое хранилище (минимум 2 ТБ).
– Контроллер домена.

Реализация FTP-сервера предусматривает обмен файлами не более определенного размера и определенных типов между учащимися или преподавателями и сервером. Важно отметить, при использовании FTP-сервера обеспечение антивирусной защиты кафедры гораздо проще. Использование антивирусного программного обеспечения на одной, мощной машине более рационально, чем на большом количестве ПК с разными конфигурациями. При этом установка антивирусной защиты на рабочих станциях не будет являться необходимой, так как вся информация, поступающая на эти машины, будет уже проверена на сервере, с помощью установленного антивируса Kaspersky security. Который позволяет проверить загружаемые файлы, исключая попадание вирусов и заражение программ и файлов. Это решает проблему передачи вредоносного ПО через съемные носители, которые являлись постоянными источниками заражения рабочих файлов и компьютеров кафедральной сети.

К преимуществам FTP-сервера можно отнести легкость при его установке и настройке. Нет необходимости использовать стороннее ПО, кроме антивирусной защиты, так как операционная система MS Windows Server обладает всеми необходимыми средствами для конфигурации. Удобство в наличии удаленного и организованного доступа. Возможность настройки прав доступа к файлам. Студенты и преподаватели могут загружать на сервер всю необходимую информацию из любого места, где есть доступ в интернет. Нет жесткого ограничения на объем. Объем дискового пространства можно быстро расширить, и как показывает практика, требуемый объем хранилища информации составляет примерно 150 ГБ на учебный семестр. С точки зрения экономических затрат покупка антивирусного ПО на 1 сервер дешевле в десятки раз, чем на все рабочие станции кафедры. На структурной схеме передачи информации с использованием FTP-сервера можно видеть, что данные загружаются в файловое хранилище кафедральной сети, это дает прямой доступ в пределах ВУЗа для дальнейшей работы с ними (рисунок 2) [3, 4]. Чего нельзя сказать при использовании облачных технологий, где необходимо с домашнего ПК загрузить файлы в облако и, в дальнейшем для работы с ними во время учебы или работы в МАДИ, вновь загрузить их из облака в файловое хранилище.

Из недостатков следует отметить относительную небезопасность протокола FTP. Однако отсутствует необходимость в использовании более серьезной защиты от взлома, кроме авторизации и аутентификации. На FTP-сервере не будут храниться личные данные студентов и преподавателей, которые могут быть скомпрометированы. Надежность FTP-сервера будет ниже, чем при использовании облачных серверов, таких как Google Drive, так как есть вероятность отключения электроэнергии или сбоев сети у поставщика Интернет. Тем не менее, при любом из возможных сбоев вся информация останется в сохранности, благодаря организации RAID массивов и теневых копий.

Как итог, можно отметить инновационность предложенного подхода.

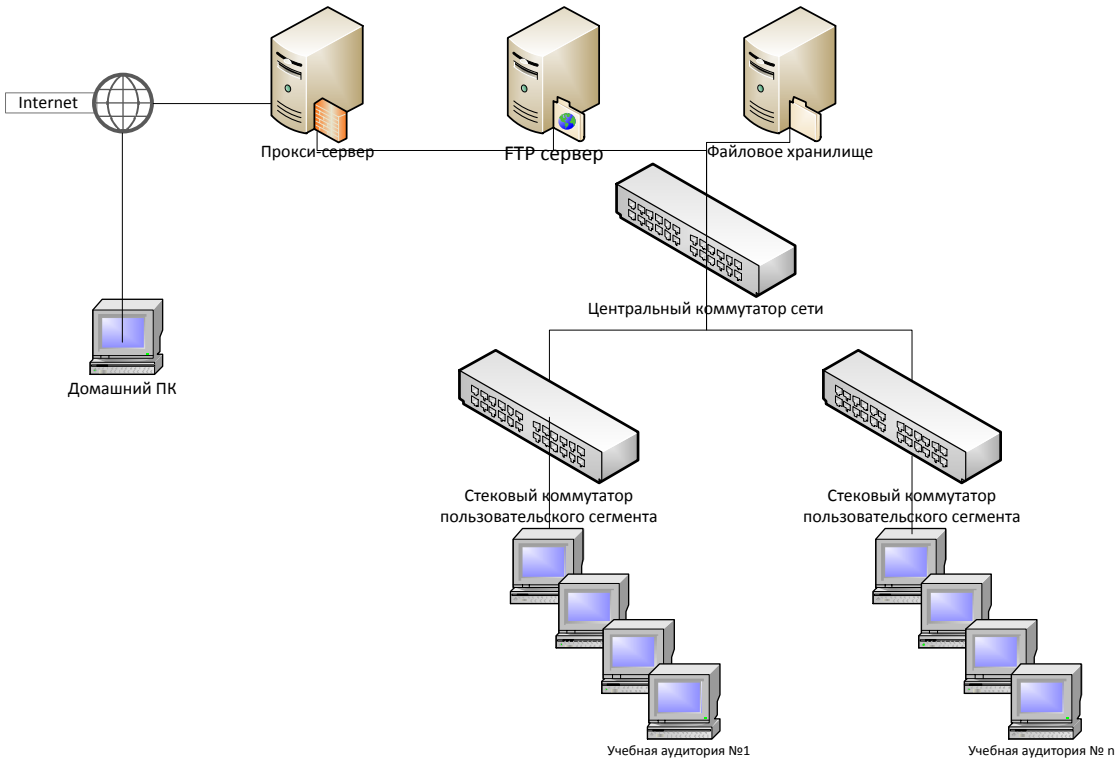

Рисунок 2 – Схема передачи данных с использованием FTP-сервера

Представление информации на FTP-сервере просто и интуитивно понятно (рисунок 3).

Рисунок 3 – Пример представления информации на FTP-сервере

4. Заключение

Проведенное сравнение средств антивирусной защиты сети показало, что каждый из предложенных решений имеет свои достоинства и недостатки, которые необходимо учитывать при решении различных задач. Для задач касающихся организации учебного процесса на кафедре АСУ МАДИ реализована система антивирусной защиты сети с использованием FTP-сервера с установленным на него антивирусом. Данный метод является оптимальным решением для обеспечения защиты информации в учебной деятельности.

В настоящее время, технология хранения информации на FTP-сервере предоставляет учащимся и преподавателям возможность:

- удобного, легкого и интуитивно понятного доступа и одновременной работы над проектами из любой точки, при помощи любого компьютера, подключенного к сети Интернет;
- значительного увеличение эффективности командной работы;
- повышения безопасности Ваших данных в несколько раз, защита от взлома, кражи и конфискации компьютеров и носителей информации;
- загрузки файлов больших объемов.

Список информационных источников

[1] Свободная энциклопедия: сайт «Википедия» [Электронный ресурс]: URL:https://ru.wikipedia.org/wiki/Компьютерный_вирус.

[2] Сайт Microsoft [Электронный ресурс]: URL:http://technet.microsoft.com

[3] Новостной сайт Habrahabr [Электронный ресурс]: URL:http://habrahabr.ru/company/epam_systems/blog/173699/.

[4] Новостной сайт Habrahabr [Электронный ресурс]: URL:http://habrahabr.ru/company/selectel/blog/213945/.

[5] Официальный сайт программы Deepfreeze [Электронный ресурс]: URL:http://www.faronics.com/en-uk/.

[6] Официальный сайт антивирусной программы AVG [Электронный ресурс]: URL:http://www.avg.com/ru-ru/internet-security-business.

[7] Остроух А.В. Ввод и обработка цифровой информации: учебник для нач. проф. образования / А.В. Остроух. – М.: Издательский центр «Академия», 2012. – 288 с. – ISBN 978-5-7695-9457-1.

[8] Сальный А.Г., Збавитель П.Ю., Николаев А.Б., Остроух А.В. Описание унифицированных программных модулей для лаборатории коллективного пользования // Автоматизация и управление в технических системах. – 2013. – № 2. – С. 12-17.

[9] Krasnyanskiy M.N., Karpushkin S.V., Obukhov A.D., Ostroukh A.V. Automated control system for university research projects // International Journal of Advanced Studies (iJAS). 2014. Vol. 4, Issue 1, pp. 22-26. DOI: 10.12731/2227-930X-2014-1-4.

[10] A.V. Ostroukh, M.N. Krasnyanskiy, S.V. Karpushkin, A.D. Obukhov. Development of Automated Control System for University Research Projects // Middle East Journal of Scientific Research. 2014. Vol. 20 (12). pp. 1780-1784. DOI: 10.5829/idosi.mejsr.2014.20.12.21091.