ОРГАНИЗАЦИЯ ЗАГРУЗКИ ОПЕРАЦИОННЫХ СИСТЕМ В КОМПЬЮТЕРНОМ КЛАССЕ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ

Воруев А. В., Левчук В. Д.

Учреждение образования «Гомельский государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В статье рассмотрено предложение об организации безопасного вычислительного процесса и регулирования профилактики компьютерных вирусов в сети учреждения образования «ГГУ им. Ф. Скорины». Описан ряд вариантов организации загрузки операционных систем из фиксированных образов, применение программных и аппаратных средств для реализации управляемой сетевой загрузки.

Введение. Основными путями проникновения вирусов в компьютеры, используемые в учебном процессе, являются сменные диски, а также компьютерные сети. Заражение жесткого диска вирусами может произойти и при загрузке программы с твердотельного накопителя, содержащей вирус. Вирус может попасть на сам носитель, даже если носитель просто подключили к системе зараженного компьютера и, например, прочитали ее оглавление.

Поскольку компьютеры, используемые в образовательном процессе, объединены в компьютерную сеть и имеют однотипные настройки операционной системы, дальнейший сценарий развития событий чаще всего попадает в схему, удобную для распространения вирусов типа *сетевой червь*.

Для решения вопросов, связанных с регулярным перезаражением операционных систем и предотвращением их несанкционированного использования в целях злоумышленников, высокую эффективность показало применение следующих технологий:

– применение «тонких клиентов»;

– реализация централизованной загрузки клиентских операционных систем.

Применение «тонких клиентов». «Тонким» клиентом или терминалом называют пользовательскую вычислительную систему, ресурсов которой недостаточно для автономной работы. В этом случае обслуживание вычислительного процесса осуществляется удаленной мощной вычислительной системой – сервером. Формализованный процесс загрузки тонкого клиента представлен на рисунке 1.

Рис. 1. Общее представление загрузки тонкого клиента

Процесс управления операционной системой тонкого клиента наиболее сложен и медлителен при работе с высоконагруженными приложениями. Но данный способ позволяет серьезно экономить на вводе новых клиентов, если им не требуется работы со сложными приложениями, например, если требуется только редактирование документов.

Тонкий клиент хорошо подходит для использования в бухгалтерии, в небольших офисах и других ситуациях, где отсутствует чувствительность к задержкам обработки запросов и соединения с оборудованием. В рассматриваемом далее примере для учебного процесса учреждения образования «ГГУ им. Ф. Скорины», требовалось создать систему для обработки информации текстового и графического содержания, компиляции программных кодов, отладки веб-приложений, управления стендами оборудования сетевых устройств L2/L3, подключения к устройствам отображения HDMI.

На рисунке 2 показан детальный процесс загрузки. Здесь добавлено новое требование, а именно загрузка учетной записи на сервер. После этого события следует передать управление на клиентскую машину. Но любые изменения требуют участия сервера. Вся основная нагрузка за выполнение приложений, работу с сетью ложится целиком на сервер. Здесь есть единственная выгода – это применение очень дешевых клиентских станций.

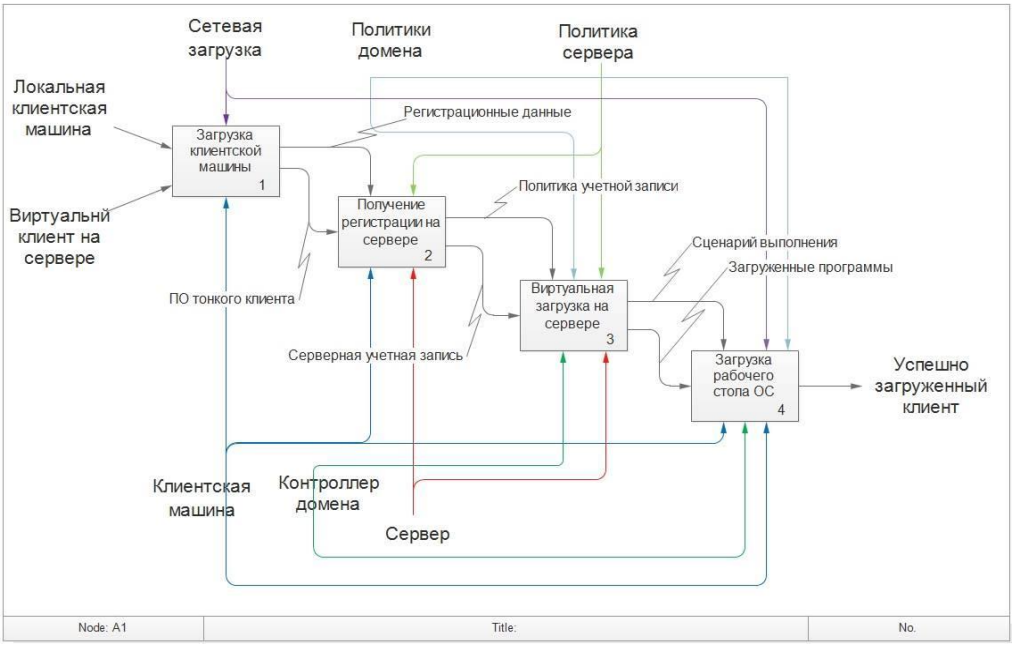

Рис. 2. Поэтапный процесс загрузки тонкого клиента

Основой смысл использования удаленной загрузки заключается в формате работы как с локальной машиной, но с использованием преимуществ тонкого клиента. Исходя из теории и практик, тонкий клиент передает выполнение задач на сервер и не требователен к машине клиента. Но в данном случае невозможно полноценно вести работу с высоконагруженными задачами, такими, как обработка графики.

Рисунок 3 показывает процесс удаленной загрузки. Для пользователя разница заключаются лишь в невозможности сохранить результат изменения системы. Т.е. несмотря на действия защиты методом запрета, у пользователя остается широкий круг возможностей.

Раньше, при реализации политики доменов в локальных машинах, требовалось ограничивать пользователей в административных правах. В данном случае этот пункт является условным. Никакие изменения, сделанные в машине, не сохранятся при последующей перезагрузке. Ограничение прав администратора имеет смысл лишь в повышении мер безопасности на сетевом уровне. Метод удаленной загрузки использует ресурсы локальной машины, т. е. производительность оборудования и нетребователен к ресурсам сервера.

В случае необходимости может быть построена модель удаленного исполнения приложений с высокой нагрузкой на вычисления, допустим, работа с базами данных. Это значит, что возможно запустить одновременно удаленную загрузку и тонкий клиент ресурсами одного

сервера. Нет смысла передавать на удаленную загрузку приложение, требовательное к вычислениям, если, конечно, для этого нет требований со стороны самих пользовательских приложений.

Как показано на рисунке 4, функционально удаленная загрузка не отличается от локальной. Для простоты процесс можно условно представить, как работу локальной машины с HDD вынесенным за ее пределы и соединенным Ethernet.

Рис. 3. Общее представление бездисковой загрузки

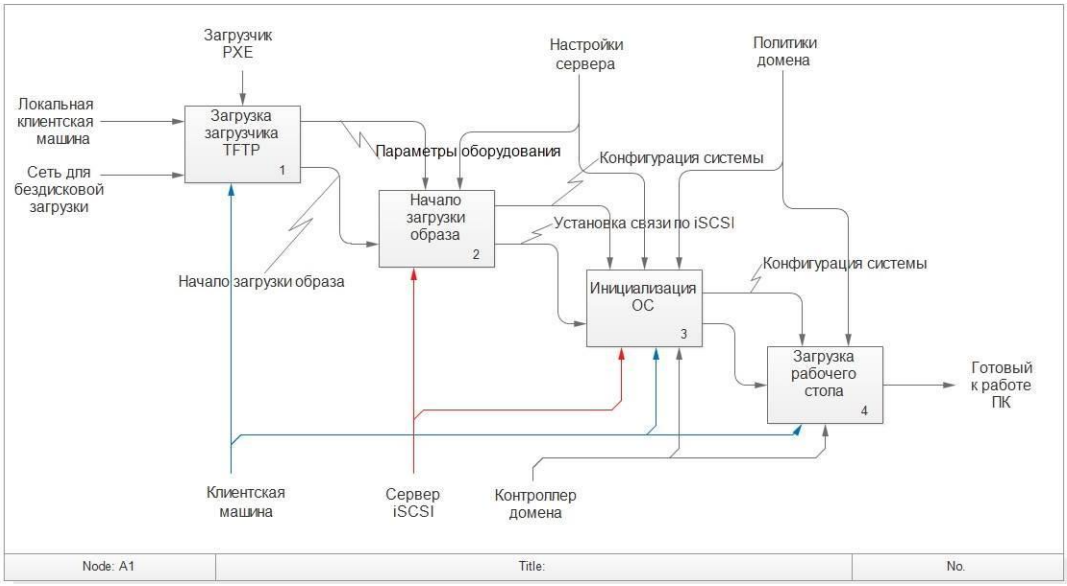

Рис. 4. Поэтапный процесс бездисковой загрузки

Низкий уровень требования к оборудованию позволяет разработчикам устройств данного типа до предела их минимизировать и компактно разместить в ограниченном объеме. Мощность, потребляемая устройствами для их работы, может быть обеспечена выносным блоком питания +5V. Также допускается использование технологии Power over Ethernet.

Превышение максимальной пропускной способности канала не приводит к сбою, а лишь вызывает замедление обновления экрана клиента. Если принять за номинальную рабочую полосу пропускания Ethernet сети 100 Мбит/сек, то данная полоса дает возможность работать либо 20-30 клиентам в режиме серьезной нагрузки без задержки обновления экрана, либо до 500 клиентов в режиме обычной офисной работы без активной динамической графики, требующей постоянной пересылки графических изображений на экран.

Пример реализации удаленной загрузки. При разработке прототипа, сеть реализации загрузки размещалась в пределах одного компьютерного класса и состояла из сервера, маршрутизатора, персональных ПК для удаленной загрузки, подключения к общей сети и раздаче сервиса Wi-Fi. Сервер использовался для задач DHCP, NAT, PXE, ISCSI. В такой схеме сер-

вер – первое из «узких мест», поскольку необходимо сохранить максимум ресурсов на основные задачи. Вторым «узким местом» является пропускная способность коммутатора, недостаток которой негативно сказывается на первичной загрузке клиентских машин. Это можно отследить на рисунке 5. В сети присутствует соединение 100 Мб/с с общей сетью и соединение 100 Мбит/сек с пользовательскими станциями. Между коммутатором и сервером канал 1 Гбит/сек. На графике видно, что даже одна пользовательская станция в такой конфигурации сети при загрузке полностью использует 100 Мбит/сек канал, т. е. всю полосу пропускания. Этот факт сказывается на скорости загрузки операционной системы – примерно от 90 до 120 секунд.

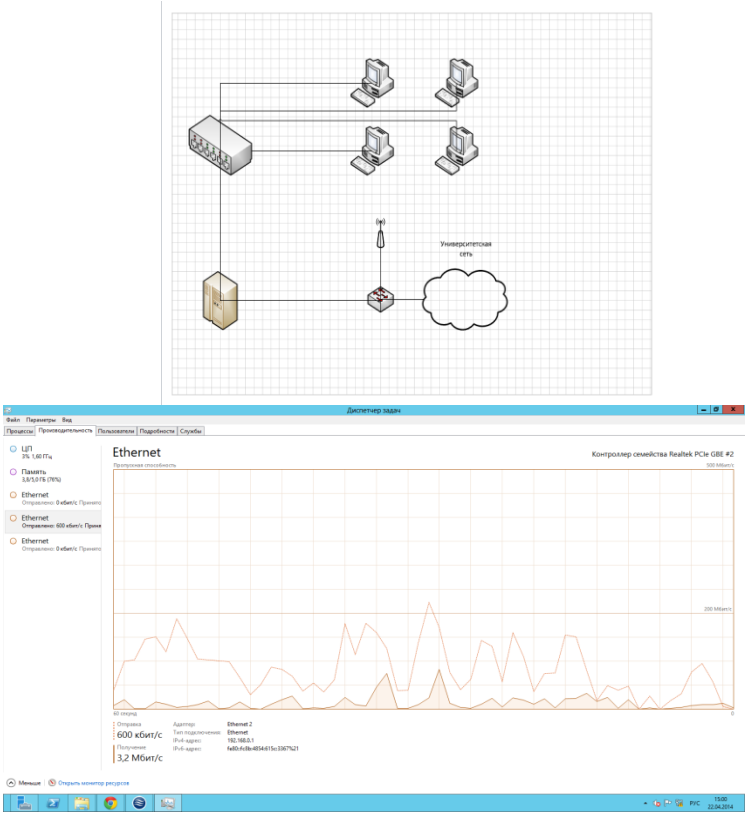

Рис. 5. График обращений к серверу при загрузке с образов в компьютерном классе

В измененной схеме (рисунок 6) сеть лишается основных недостатков. Надобность в промежуточном NAT преобразовании сетевых пакетов отпадает, что освобождает ресурсы сервера. За разделение и передачу трафика между VLAN отвечает маршрутизатор Mikrotik CRS125-24G-1S-2HnD-IN. Каналы связи на всех участках сети поддерживают скорость 1 Гбит/сек. Маршрутизатор также является точкой Wi-Fi.

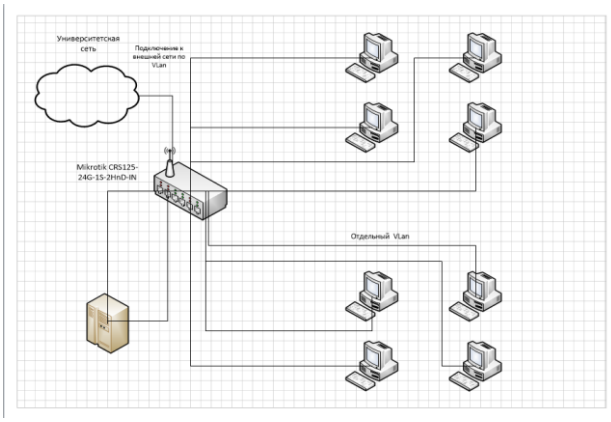

Рис. 6. Изменение компоновки сети с переносом части функций на сетевое устройство

По сравнению с первой реализацией на сервере сохраняется только нагрузка сервисов DHCP, PXE и самого ISCSI. С помощью MikroTik Router OS возможно как производить

VLAN-маркировку кадров данных, так и принимать, и маршрутизировать пакеты. Поскольку VLAN функционирует на втором уровне OSI, то данную структуру можно использовать точно так же, как и любой другой сетевой интерфейс без каких-либо ограничений. VLAN успешно проходит через обычные Ethernet-сетевые мосты.

Также возможно пустить VLAN по беспроводным каналам и задействовать несколько VLAN-интерфейсов на одном беспроводном интерфейсе. Необходимо иметь в виду, что, поскольку VLAN не является в полной мере туннельным протоколом, то при организации сетевого моста между VLAN, к нему применимы те же ограничения, что и при организации сетевого моста между простыми беспроводными интерфейсами. Иными словами, до тех пор пока беспроводные клиенты являются участниками VLAN, размещенных на беспроводных интерфейсах, невозможно разместить VLAN на беспроводном интерфейсе, находящимся в режиме станции, объединенным в сетевой мост с любым другим интерфейсом.

В компьютерном классе VLAN выполняет функцию логического разделения. Каждая аудитория или группа узлов локализуется как отдельная сеть. Для реализации этой части настроек используется следующая последовательность команд:

– создаем VLAN интерфейсы:

```
/interface VLAN
add name=VLAN2 VLAN-id=2 interface=ether1 disabled=no
add name=VLAN3 VLAN-id=3 interface=ether1 disabled=no
```

– контролируем реакцию системы:

```
[admin@MikroTik] /interface VLAN> add name=VLAN2 VLAN-id=2 interface=ether1
disabled=no
[admin@MikroTik] /interface VLAN> print
Flags: X - disabled, R - running, S - slave
#    NAME        MTU   ARP         VLAN-ID INTERFACE
0 R  VLAN2        1500  enabled     2       ether2
0 R  VLAN3        1500  enabled     2       ether3
```

– присваиваем интерфейсам SVI IP-адреса:

```
/ip address
add address= 192.168.2.0/24 interface=VLAN2
addaddress= 192.168.3.0/24 interface=VLAN3
```

– контролируем реакцию системы:

```
[admin@MikroTik] ip address> add address=192.168.2.1/24 interface=VLAN2
[admin@MikroTik] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
#    ADDRESS         NETWORK      BROADCAST    INTERFACE
0   192.168.1.1/24   192.168.1.0  10.0.1.255     ether1
1   192.168.2.1/24   192.168.1.0  10.20.0.255    VLAN2
2   192.168.3.1/24   192.168.1.0  10.04.10.255   VLAN3
[admin@MikroTik] ip address>
```

На рисунке 7 представлен график загрузки операционной системы клиента после изменения схемы сети.

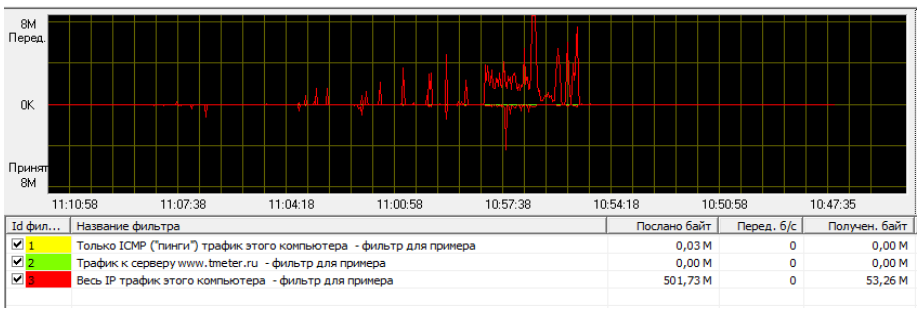

Рис. 7. Статистика загрузки канала после изменения топологии