ДОСТИЖЕНИЕ ПОВЫШЕННОЙ ОТКАЗОУСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ «СЕТЕВОЙ ГОРОД. ОБРАЗОВАНИЕ»

Деменко Инга Николаевна (inga1961@bk.ru), Департамент образования администрации г. Южно-Сахалинска
Клинов Алексей Александрович (a.klinov@adm.sakhalin.ru), Министерство образования Сахалинской области

Аннотация

В докладе описывается модель реализации системы «Сетевой Город. Образование», при которой решаются следующие проблемы: с неустойчивыми и низкоскоростными каналами связи; высокой стоимостью каналов связи; с высокой готовностью и безопасностью информационной системы.

1. Каналы связи, надёжность и высокая доступность

Реализация системы NetSchool локально в образовательном учреждении, как правило, достаточно проста с технической точки зрения ввиду относительной надёжности школьной ЛВС. При переходе к системе «Сетевой Город. Образование», по схеме с одним центральным сервером, возникает необходимость в наличии надёжного канала связи, с дополнительным резервированием.

В г. Южно-Сахалинске сложность состояла в дороговизне выделенных каналов связи, предоставляемых местными провайдерами, и зачастую в физической невозможности обеспечить резервные каналы.

Поэтому при построении системы «Сетевой Город. Образование» в г. Южно-Сахалинске было принято во внимание, что все 31 общеобразовательных учреждения уже находятся в единой IP-VPN сети «Образование», при помощи которой они имеют доступ в сеть Интернет. Анализ имеющихся каналов связи показал их малую надёжность и низкую пропускную способность, что вкупе с отсутствием возможности создания резервных каналов связи вынудило к поиску компромиссного решения. Решением стало создание распределенной системы локальных серверов в образовательных учреждениях и центрального сервера, расположенного в Министерстве образования Сахалинской области. Практически в каждом образовательном учреждении г. Южно-Сахалинска, за исключением нескольких небольших образовательных учреждений, был установлен локальный сервер «Сетевой Город. Образование». Небольшие учреждения, наоборот, работают по стандартной схеме, на центральном сервере. Также по стандартной схеме, на центральном сервере, имеют возможность работать сотрудники Департамента образования г. Южно-Сахалинска.

Высокая доступность обеспечивается возможностью работы образовательных учреждений, имеющих собственный локальный сервер, также и непосредственно на центральном сервере. Такой режим работы может временно потребоваться в случае выхода из строя локального сервера в образовательном учреждении. После восстановления локального сервера происходит обратная репликация базы данных образовательного учреждения, и далее работа с системой «Сетевой Город. Образование» происходит в штатном режиме, на локальном школьном сервере.

Учитывая перспективы дальнейшего масштабирования системы, физически расположение центрального сервера было определено в Министерстве образования Сахалинской области. Центральная система подключается к IP-VPN сети «Образование» посредством 2 Мбит/с канала связи, организация которого с 2010 года является обязательным условием выполнения государственного контракта по предоставлению доступа в сеть Интернет для образовательных учреждений. Департамент образования г. Южно-Сахалинска также подключен к IP-VPN сети «Образование» по отдельному договору с провайдером связи. Такая возможность, как

подключения дополнительных объектов, также предусмотрена в государственном контракте на предоставление доступа в сеть Интернет в 2010 г. Условия контракта планируется выдерживать и в дальнейшем, для обеспечения бесперебойного функционирования системы. По подобной схеме подключения к системе «Сетевой Город. Образование» предусматривается дальнейшее расширение системы на другие муниципальные образования Сахалинской области. Так, в этом году запланировано внедрение системы «Сетевой Город. Образование» в Углегорском р-не Сахалинской области.

Технические решения, обеспечивающие высокую надёжность и доступность сервиса:

1.1. Агрегирование информации на центральном сервере производится путем двухсторонней репликации баз данных между локальными серверами в образовательных учреждениях и центральной системой в Министерстве образования. Для обеспечения оптимальной скорости репликация баз данных производится в нерабочее время суток, ночью.

1.2. На физическом уровне высокая надёжность центральной части системы обеспечивается дублированием всех элементов, составляющих её аппаратную часть. Отдельного упоминания заслуживает применение технологии виртуализации на базе программного обеспечения ESX от VMware, обеспечивающей высокую гибкость при управлении вычислительными ресурсами виртуальных серверов. Применение виртуализации также обеспечило аппаратную развязку виртуальных машин от применяемого оборудования, что оперативно решает практически все проблемы совместимости при необходимости замены серверного оборудования.

1.3. Для обеспечения сохранности данных дополнительно применяется система резервного копирования Symantec Backup Exec. Данная система производит ежедневное получение резервных копий виртуальных серверов, с возможностью дальнейшего оперативного восстановления.

2. Информационная безопасность

Изначально, ещё на самых ранних этапах знакомства с системой NetCity, было обращено пристальное внимание на аспекты информационной безопасности при обработке информации, в том числе и защиты от возможной несанкционированной модификации данных пользователей. Данные аспекты являются жизненно важными, если рассматривать информационную систему в качестве первичной системы документооборота. Ещё более ситуация обострилась с появлением 152 ФЗ «О персональных данных» и сопутствующих нормативных документов, регламентирующих применяемые меры по предотвращению реализации потенциальных угроз для информационной системы «Сетевой Город. Образование».

При рассмотрении возможных угроз были выделены следующие:

2.1. Угроза несанкционированного доступа с целью искажения или уничтожения информации

Решением проблемы стало использование генераторов одноразовых паролей eToken PASS производства компании Aladdin. Привлекательность данного решения обусловлена простотой применения средств аутентификации со стороны пользователя, длительным сроком службы (7 лет или 14000 генераций), компактными размерами устройства и отсутствием необходимости подключения устройства к ПК и установки какого-либо программного обеспечения. Для оптимальной функциональности произведена глубокая интеграция eToken PASS с системой «Сетевой Город. Образование», позволившая встроить все необходимые элементы управления ключами eToken PASS в web-интерфейс системы.

В результате система «Сетевой Город. Образование» получила дополнительную возможность по аутентификации пользователей системы, являющуюся достаточно надёжным средством защиты от НСД. В настоящий момент использование eToken PASS является обязательным для сотрудников образовательных учреждений и Департамента образования г. Южно-Сахалинска. При необходимости или желании любой пользователь может использовать аутентификацию в системе посредством eToken PASS. Для учеников и родителей существует возможность эксплуатации единственного генератора eToken PASS в расчёте на семью, так называемый «семейный вход», позволяющий не приобретать генератор персонально для каждого пользователя.

2.2. Угроза утечки конфиденциальной информации при передаче её по каналам связи между сервером образовательного учреждения и центральным сервером

Ввиду того, что при репликации происходит передача данных вне пределов контролируемых зон, возникла необходимость защиты передаваемой информации от возможного перехвата. Задача решена применением программных комплексов – S-Terra CSP VPN Gate 100, представляющих собой функционирующий на аппаратной платформе шлюз безопасности под управлением ОС Red Hat Linux 9 в образовательных учреждениях, Департаменте образования г.Южно-Сахалинска, а также программных комплексов S-Terra CSP VPN Gate 3000, представляющих собой шлюз безопасности, функционирующий на аппаратной платформе под управлением операционной системы Sun Solaris 9 в Министерстве образования Сахалинской области. Применение данных средств позволяет обеспечивать защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP.

Все применяемые средства имеют действующие сертификаты ФСТЭК и ФСБ, согласно которым обеспечивается необходимый уровень защиты при применении данных средств защиты информации.

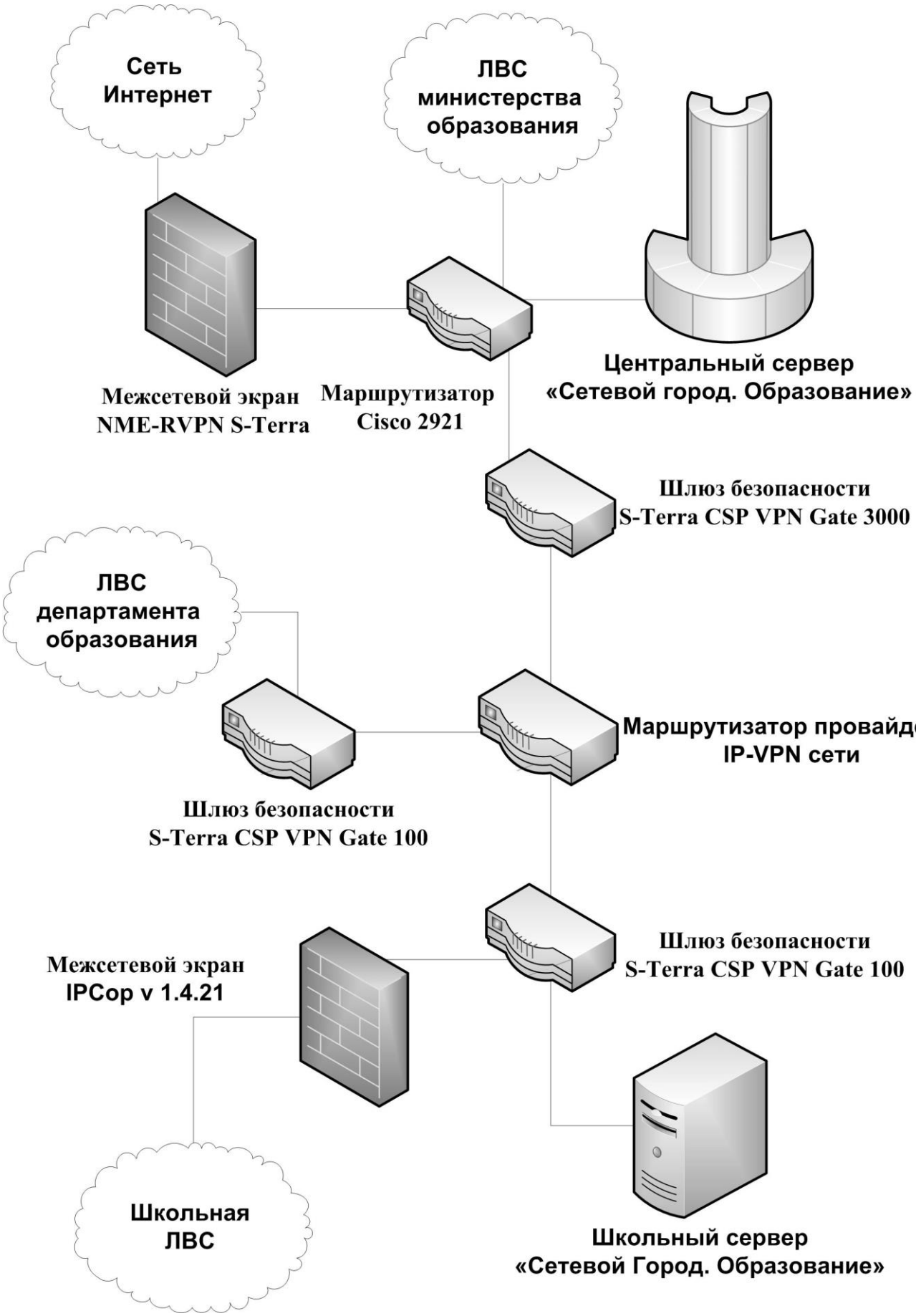
2.3. Угроза несанкционированного доступа из сети Интернет к элементам системы с целью изменения, уничтожения обрабатываемых в информационной системе данных

На настоящий момент система «Сетевой Город. Образование» не имеет возможности доступа из внешних небезопасных сетей. Но ввиду насущной необходимости иметь таковой доступ данная задача будет решена до конца сентября нового, 2010, учебного года.

Решение базируется на применении сертифицированного оборудования: маршрутизатора Cisco 2921 и модуля для организации сертифицированного межсетевого экрана NME-RVPN S-Terra. В результате ввода в эксплуатацию данного оборудования ожидается обеспечение удовлетворительного уровня безопасности системы «Сетевой Город. Образование» при доступе к ней из сети Интернет. Также, после внедрения системы безопасности и подключения к сети Интернет, будет произведено подключение системы к сервису рассылки СМС-сообщений.

Таким образом, в итоге получена масштабируемая система с повышенной надёжностью и доступностью, защищённая сертифицированными средствами обеспечения безопасности при передаче данных и защитой от НСД.

На 2010-2013 годы запланировано дальнейшее развитие системы в масштабах Сахалинской области. Предложения по финансированию проекта включены в перечень мероприятий построения «Информационного сообщества на 2011-2013 годы» и проходят процедуру утверждения. Дальнейшее развитие системы видится в расширении охвата разнотипных образовательных учреждений, реализации различных дополнительных возможностей.


Сеть
Интернет
ЛВС
министерства
образования
Межсетевой экран
NME-RVPN S-Terra
Маршрутизатор
Cisco 2921
Центральный сервер
«Сетевой город. Образование»
Шлюз безопасности
S-Terra CSP VPN Gate 3000
ЛВС
департамента
образования
Маршрутизатор провайдера
IP-VPN сети
Шлюз безопасности
S-Terra CSP VPN Gate 100
Межсетевой экран
IPCop v 1.4.21
Шлюз безопасности
S-Terra CSP VPN Gate 100
Школьная
ЛВС
Школьный сервер
«Сетевой Город. Образование»