УДК 004.056

М.А. Сопов, С.В. Тимченко, В.В. Кручинин, М.В. Чуркин, А.А. Шелупанов

Защищенная информационно-технологическая платформа виртуальных серверов удостоверяющих центров

Предложена модель функционирования серверов удостоверяющих центров на базе информационно-технологической платформы. Показывается эффективность работы данной конфигурации с одновременным повышением надежности функционирования.
Ключевые слова: удостоверяющий центр, электронная подпись, модель функционирования, виртуальный сервер.

Виртуальные машины прочно заняли свое место среди инструментов, существенно повышающих эффективность использования серверных платформ и персональных компьютеров. Возможность консолидации нескольких виртуальных серверов на одном физическом позволяет организациям различного уровня существенно экономить на аппаратном обеспечении и обслуживании [1]. Пользователи настольных компьютеров применяют виртуальные машины как в целях обучения, так и в целях создания защищенных и переносных пользовательских сред. В корпоративной среде виртуальные машины на настольных системах применяются также для целей тестирования программного обеспечения в различных конфигурациях, запуска специализированных виртуальных шаблонов и централизованного хранения виртуальных пользовательских десктопов [2]. При массовом использовании виртуальных систем одними из самых важных мероприятий являются обслуживание и оптимизация производительности виртуальных машин. В то время как большинство производителей платформ виртуализации предоставляют пользователям и системным администраторам множество инструментов и средств для поддержания эффективной виртуальной инфраструктуры, оптимизация производительности как самих платформ, так и виртуальных машин является более тонким моментом. Применение различных техник оптимизации во многом зависит от используемой платформы, вариантов использования виртуальных машин, доступных средств и квалификации персонала.

С течением времени требования к автоматизации деловых процессов растут. И если когда-то ставилась задача автоматизации отдельных участков работы подразделений, что привело к наличию большого количества разрозненных программных продуктов, то теперь основной вопрос – организация комплексной системы оперативного управления. Именно этот подход позволяет наиболее эффективно решить задачу автоматизации.

Структура УЦ

Основной задачей удостоверяющего центра (УЦ, СА) является удостоверение соответствия открытого ключа подписи/шифрования закрытому ключу, а также подтверждение достоверности регистрационного свидетельства.

Удостоверяющим центром в установленном законодательством порядке осуществляются в пределах своей компетенции следующие функции:

1) первичная регистрация, формирование личных (закрытых) и открытых ключей и регистрационных свидетельств пользователей;

2) выдача, хранение регистрационных свидетельств;

3) выпуск, приостановление/возобновление действия, отзыв (аннулирование) регистрационных свидетельств;

4) публикация списка отозванных регистрационных свидетельств в регистре;

5) ведение регистра (каталога) регистрационных свидетельств;

6) подтверждение принадлежности, подлинности и действительности регистрационного свидетельства открытого ключа.

Цифровые сертификаты представляют собой эффективное средство определения подлинности, которое можно применять при аутентификации пользователей в процессе регистрации, для обеспечения безопасного обмена информацией в Internet и определения происхождения программного

обеспечения. Одной из главных областей применения цифровых сертификатов является шифрование данных и электронная подпись сообщений электронной почты. С помощью последней получатели письма могут удостовериться, что письмо было послано именно данным отправителем и не изменено [3].

В основе технологии управления доверительными отношениями как между центрами CA, так и между пользователями инфраструктуры PKI и центрами сертификации лежит понятие модели доверия PKI. Домен доверия CA представляет собой структуру, определяющую те организационные или географические границы, в пределах которых находятся только заслуживающие доверия центры CA. В рамках одной организации может существовать несколько различных доменов доверия, что может соответствовать, например, структурному делению организации на подразделения и департаменты. Для всех пользователей PKI в домене доверия CA удостоверяющий центр рассматривается как центр доверия, которому пользователь PKI может доверять при любых обстоятельствах. В процессе проверки подлинности сертификата программное обеспечение PKI пытается выстроить путь доверия до уровня корневого CA, который является центром доверия [4].

Инфраструктура Windows Server 2003 PKI поддерживает две основные модели доверительных отношений: иерархическую и сетевую. Кроме того, существует возможность установления регулируемых ограниченных доверительных отношений, что позволяет администратору модифицировать доверительные отношения между центрами CA.

Сетевая модель

В сетевой модели доверительных отношений (также называемой моделью «точка-точка» (P2P) или распределенной моделью доверительных отношений) между центрами CA отсутствуют отношения типа «вышестоящий – подчиненный», здесь все центры сертификации рассматриваются как равноправные точки. Данная модель обычно используется в PKI при установлении доверительных отношений между организациями. В модели P2P существует два метода установления доверительных отношений: с помощью списков сертификатов, заслуживающих доверия (Certificate Trust List, CTL), и кросс-сертификатов. Инфраструктура Windows 2003 PKI поддерживает оба метода.

Список CTL представляет собой заверенный перечень сертификатов, которым доверяет центр CA. Администратор PKI осуществляет централизованное управление этим списком и распространяет его по всем клиентам инфраструктуры PKI организации. Списки CTL могут быть определены с помощью установки параметров объекта групповой политики (GPO). В инфраструктурах PKI систем Windows 2003 и Windows 2000 можно задавать срок действия CTL, а также ограничивать его применение определенным набором приложений, работающих с PKI.

Рис. 1. Сетевая модель прямого доверия

Кросс-сертификация представляет собой не что иное, как возможность обмена сертификатами между двумя центрами CA, которые являются точками в сетевой модели доверительных отношений, т.е. один центр CA может выдавать сертификат другому центру и, соответственно, получать от него сертификат. При кросс-сертификации допускаются как односторонние, так и двусторонние доверительные отношения (т.е. когда оба CA могут сертифицировать друг друга). Пример построения доверительных отношений между организациями в соответствии с сетевой моделью показан на рис. 1.

В клиентах PKI систем Windows 2003 и Windows XP реализована поддержка механизмов обнаружения путей доверия и отслеживания связей, необходимых для построения сетевой модели доверительных отношений с несколькими связями кросс-сертификации. В клиентах PKI системы Windows 2000 такие механизмы не поддерживаются. При проверке подлинности сертификата, выданного центром CA, который является точкой сетевой модели, программное обеспечение PKI клиента пытается выстроить путь доверия, который связывает центр CA, выдавший сертификат, с центром доверия локального CA.

Иерархическая модель

Количество и уровни CA должны учитывать сразу, в зависимости от требований к безопасности и доступности. Должны постараться организовать вашу иерархию в соответствии с вашими нужда-

ми. В действительности не существует каких-либо рекомендаций относительно того, сколько уровней СА нужно, хотя очень редко кому-либо необходимо 4 уровня или более. Однако существует правило «большого пальца», которое представлено в табл. 1, и которое поможет идти в верном направлении.

Таблица 1

Характеристики иерархии СА

Уровень СА	Комментарии
	Низкая безопасность (Low security). Сниженные требования к безопасности СА. Состоит из одного корневого СА. Небольшое количество запросов сертификатов
	Средняя безопасность (Medium security). Состоит из автономного (offline) корневого и оперативных (online) второстепенных СА. Автономный СА удаляется из сети. Оперативные СА остаются в сети. Рекомендуется использовать два или более СА для выпуска каждого шаблона для сертификата
	Высокая безопасность (High security). Состоит из автономного корневого (offline root) и автономной политики (offline policy). Один или более выпускающих оперативных дополнительных СА. Подходит для больших географически разнесенных организаций

Практическая реализация иерархической модели

Для реализации трёхуровневой модели понадобится 3 сервера Windows Server 2003 и 1 клиентская машина Windows XP. Чтобы построить трёхуровневую модель, в качестве корневого СА будет использован «изолированный корневой ЦС» (1-й уровень). В качестве промежуточного СА будет использоваться «изолированный подчинённый УЦ» (2-й уровень). В качестве выпускающего СА 3-го уровня будет выступать «подчинённый УЦ предприятия». В табл. 2 приведены параметры настройки серверов.

Таблица 2

Параметры настройки серверов для трехуровневой иерархической модели

Параметр	Корневой СА	Промежуточный СА	Выпускающий СА
Имя сервера	Server	Server-RA	Server-RA-2
Тип СА	Изолированный корневой	Изолированный подчиненный	Корпоративный подчиненный СА
CSP	Microsoft Base Провайдер	Microsoft Base Провайдер	Microsoft Base Провайдер
Алгоритм хеширования	SHA-1	SHA-1	SHA-1
Длина ключа	4096	2048	1024
Имя СА	Root-CA	First-RA	Second-RA
Период действия (через графический интерфейс)	20 лет	N/A	N/A
Период действия (параметры реестра)	10 лет	5 лет	Не изменяется
Родительские СА	N/A	Root-CA	First-RA

Отозванные сертификаты

Возникают ситуации, когда по каким-либо причинам действие электронного сертификата лица, пользующегося услугами УЦ, приостанавливается либо прекращается. В этом случае ЦУ помещает серийный номер данного сертификата в список отозванных сертификатов и затем его публикует на своем сайте. Каждый список отозванного сертификата имеет свой интервал публикации, в течение которого его можно применять для проверки цепи доверия.

При выстраивании цепи доверия необходимо, чтобы на Вашей рабочей станции был установлен действующий список отозванных сертификатов. Файл списка отозванных сертификатов имеет расширение *.crl

Как уже не раз говорилось, иерархическая модель, состоящая из нескольких уровней: корневой (1-й уровень), промежуточный (2-й уровень) и выпускающий УЦ (3-й уровень) – наиболее безопасна. Но не стоит забывать: если корневой ЦС будет скомпрометирован, повреждён или утерян, то необходимо будет заново выдавать все сертификаты безопасности и сменить собственный. Это был рассмотрен самый худший вариант. Если же будет скомпрометирован 2-й уровень, то необходимо будет обновить сертификат скомпрометированного промежуточного УЦ и все сертификаты выданные выпускающим УЦ и их пользователям. Если же скомпрометирован 3-й уровень, то необходимо будет сменить сертификат скомпрометированного выпускающего УЦ и все сертификаты, выданные им.

Определимся с основными характеристиками, по которым будем осуществлять выбор программной платформы: функциональность, скорость загрузки гостевой ОС, скорость работы гостевой ОС, количество поддерживаемых виртуальными системами видов ОС и архитектур, техническая поддержка.

Функциональные возможности виртуальных машин

В России наиболее популярными средствами виртуализации являются продукты компании VMware. Поэтому для анализа возьмём 2 продукта компании VMware: Workstation и Server. Чтобы анализ не выглядел однонаправленным, возьмём разработку компании Microsoft продукт Virtual PC. Определим ряд функциональных возможностей для этих систем (табл. 3).

Таблица 3

Функциональные возможности средств виртуализации

Возможности	Workstation 6.5.2	Server 2.0.2	Virtual PC
1	2	3	4
Запуск в качестве сервиса	Нет (но есть возможность сворачивания UI в System Tray)	Да	Нет
Запуск виртуальной машины при загрузке	Нет	Да	Нет
Кроссплатформенность	Да	Да	Нет
Локальное управление	Толстый клиент, командная строка	Толстый клиент, командная строка	Да
Множественный пользовательский доступ	Нет	Да	Нет
Программные интерфейсы	C / COM / Perl	C / COM / Perl	C / COM
Удаленное управление хостом	Нет	Web-консоль	Нет
Удаленное управление виртуальными машинами	Нет	Толстый клиент	Нет
Управление множественными установками	Нет	Нет	Нет
Соотношение виртуальных машин на ядро	2–4	2–4	2-4
Поддержка аппаратной виртуализации	Intel VT	Intel VT (экспериментально)	Есть
Поколение виртуального аппаратного обеспечения	6	5	?
Виртуальных процессоров через SMP (Symmetric Multi Processing)	2	2 (экспериментально)	?
Максимум оперативной памяти для одной виртуальной машины	до 8 Гб	до 3,6 Гб	?
Максимум оперативной памяти для всех виртуальных машин	Неограниченно	До 64 Гб	?
IDE контроллеров/дисков на них	¼	¼	½
SCSI контроллеров/дисков на них	1/60	4/60	Нет
Максимальный размер виртуального диска (IDE/SCSI)	до 950 Гб	до 950 Гб	+/–

Продолжение табл. 3

1	2	3	4
Виртуальных сетевых адаптеров на одну виртуальную машину	10	4	?
Виртуальных коммутаторов	10	9	?
Снапшоты через толстый клиент	Да	Да (только один)	Нет
Снапшоты через командную строку	Да	Нет	Нет
Клонирование виртуальных машин	Да	Нет	Нет
Команды виртуальных машин (в одном виртуальном сетевом сегменте)	Да	Нет	Нет
Запись активности виртуальной машины	Да	Нет	Нет
Отладка виртуальных машин	Да	Да	Нет
Общие папки с хостовой системой	Да	Нет	Нет
Официально неподдерживаемые хостовые системы	SuSE Linux 7.3	Windows XP Professional (32/64 бит) Windows XP Home Windows 2000 Professional Red Hat Linux 7.0 Red Hat Linux 7.1	Все, кроме Windows XP и более поздних версий
Поддержка 64-битных систем	Да	Да	Да
Запись активности виртуальной машины в видеофайл	Да	Нет	Нет
Интерфейс Drag&Drop между гостевой и хостовой системой	Да	Нет	Нет
Поддержка паравиртуализации	Да	Нет	Нет
Поддержка ускорителя 3D	Да	Да	Нет

После завершения первого этапа можно сделать первые выводы. VMware, являясь одним из старейших участников рынка, на данный момент является его лидером и во многом определяет направления развития сферы виртуализации в целом. Сегодня день наибольший интерес для пользователей представляют коммерческие платформы VMware Workstation и бесплатная платформа VMware Server. Несмотря на то, что VMware Server является серверной платформой, многие пользователи успешно применяют ее в качестве настольной платформы ввиду ее бесплатности, хотя практически по всем параметрам функциональность продукта VMware Workstation 6 намного выше. Рассматривая продукт Microsoft Virtual PC, можно сделать вывод, что он подходит к использованию в домашних условиях для решения проблем совместимости новых ОС Windows 7 и Vista с Windows XP к примеру. По большому счёту это система не подойдёт, даже если взять весьма существенные особенности, к примеру, создание снапшотов, то Virtual PC их не поддерживает, или восстановление после сбоя, т.е. информация безвозвратно потеряна, что повлечёт за собой большие финансовые потери.

Скорость загрузки ОС на виртуальной машине

Программа сама определяет рекомендуемые параметры: минимум, максимум и стандарт. Изменяя объём памяти и число ядер процессора, проведём тест и посмотрим, как эти параметры будут влиять на быстроту загрузки ОС. В качестве ОС была выбрана продукция Microsoft, Windows Server 2003 Standard Edition. Для начала проведём тестирование VMware Workstation, результаты представлены в табл. 4.

Как видно из результатов тестирования, параметры, которые были заявлены как рекомендуемые, в настройках Workstation оказались действительно оптимальными, поскольку меньший объём оперативной памяти даёт весьма плохие результаты тестов (строки 1, 2, 5, 6 табл. 4), а повышение объёма ненамного поднимают скорость загрузки (строки 4, 8 табл. 4).

Проведём аналогичный тест для виртуальной платформы VMware Server, для того чтобы эксперимент был действительно результативным, будет использована та же ОС Windows Server 2003 Standard Edition с аналогичными настройками. Поскольку фирма VMware реализовала поддержку образов, создаваемых различными продуктами виртуализации, то не составит большого труда образ, использованный в Workstation, использовать и в VMware Server. Результат теста представлен в табл. 5.

Таблица 4

Результаты тестирования VMware Workstation

Тест	Память	Процессор	Используется памяти (до загрузки), Мб	Используется памяти (после загрузки)	Используемая память, Мб	Время загрузки ОС
1	64 Мб	1	740	980 Мб	240	8 мин 20 с
2	128 Мб	1	550	855 Мб	305	5 мин 9 с
3	384 Мб	1	550	1,10 Гб	550	4 мин 36 с
4	1 Гб	1	667	1,80 Гб	1133	4 мин 38 с
5	64 Мб	2	644	907 Мб	263	6 мин 48 с
6	128 Мб	2	640	973 Мб	333	4 мин 58 с
7	384 Мб	2	646	1,21 Гб	564	2 мин 38 с
8	1 Гб	2	632	1,81 Гб	1178	2 мин 34 с

Таблица 5

Результаты тестирования VMware Server

Тест	Память	Процессор	Используется памяти (до загрузки)	Используется памяти (после загрузки), Гб	Используемая память, Мб	Время загрузки ОС
1	64 Мб	1	1,05 Гб	1,31	260	6 мин 48 с
2	128 Мб	1	1,06 Гб	1,40	340	4 мин 58 с
3	384 Мб	1	875 Мб	1,44	565	4 мин 50 с
4	1 Гб	1	743 Мб	1,90	1157	4 мин 52 с
5	64 Мб	2	790 Мб	1,05	260	7 мин 00 с
6	128 Мб	2	803 Мб	1,15	347	5 мин 05 с
7	384 Мб	2	816 Мб	1,42	604	4 мин 41 с
8	1 Гб	2	702 Мб	1,90	1198	4 мин 45 с

Из результатов тестирования видно, что VMware Server значительно уступает VMware Workstation. Проведём анализ результатов по скорости загрузки продуктов компании VMware. Результаты сравнений представлены в табл. 6.

Таблица 6

Сравнение результатов работы VMware Server и VMware Workstation

Тест	Память	Процессор	Используемая память Workstation, Мб	Используемая память Server, Мб	Время загрузки ОС на Workstation	Время загрузки ОС на Server
1	64 Мб	1	240	260	8 мин 20 с	6 мин 48 с
2	128 Мб	1	305	340 Мб	5 мин 9 с	4 мин 58 с
3	384 Мб	1	550	565 Мб	4 мин 36 с	4 мин 50 с
4	1 Гб	1	1133	1157 Мб	4 мин 38 с	4 мин 52 с
5	64 Мб	2	263	260 Мб	6 мин 48 с	7 мин 00 с
6	128 Мб	2	333	347 Мб	4 мин 58 с	5 мин 05 с
7	384 Мб	2	564	604 Мб	2 мин 38 с	4 мин 41 с
8	1 Гб	2	1178	1198 Мб	2 мин 34 с	4 мин 45 с

При сравнении видно, что потребляемая память обеими виртуальными машинами практически одинакова, но совсем иначе обстоят дела со временем загрузки ОС. У VMware Server быстродействие с увеличение числа ядер существенно не изменяется.

Скорость работы гостевой ОС

Для обеспечения оптимального быстродействия гостевой ОС нужно использовать только необходимое ПО. В качестве теста установим программу Microsoft Word 2007. В таблице ниже представлены тесты времени установки и проверки на наличие вирусов, червей, троянских программ (табл. 7).

Таблица 7

Результаты тестирование прикладного программного обеспечения

Тест	Память	Процессор	Платформа	Время установки Microsoft Word
1	64 Мб	1	–	–
2	128 Мб	1	VMware Workstation	11 мин 5 с
3	384 Мб	1	VMware Workstation	4 мин 2 с
4	1 Гб	1	VMware Workstation	3 мин 32 с
5	64 Мб	2	–	–
6	128 Мб	2	VMware Workstation	11 мин 30 с
7	384 Мб	2	VMware Workstation	4 мин 10 с
8	1 Гб	2	VMware Workstation	3 мин 50 с
9	64 Мб	1	–	–
10	128 Мб	1	VMware Server	8 мин 34 с
11	384 Мб	1	VMware Server	4 мин 46 с
12	1 Гб	1	VMware Server	4 мин 16 с
13	64 Мб	2	–	–
14	128 Мб	2	VMware Server	5 мин 8 с
15	384 Мб	2	VMware Server	4 мин 13 с
16	1 Гб	2	VMware Server	4 мин 20 с

VMware Server несколько уступает по быстродействию, но зато из результатов видно, что Server работает более стабильно даже с меньшим объёмом памяти, установка занимает не так много времени, как на VMware Workstation. С пользовательской стороны работать с Server было намного удобнее, нежели с Workstation. Также очень удобна консоль, позволяющая закрывать графическую оболочку гостевой ОС Server, не останавливая работу самого сервера, чего не было в Workstation. Это позволяет сберечь графические ресурсы. Итак, почему же выбор остановился на VMware Server? Подытожим всё, что было сказано выше. Создавая и запуская виртуальные машины с помощью VMware Server, пользователи могут:

– инициализировать дополнительные серверы за считанные минуты, не вкладывая средства в новое оборудование;

– запускать операционные системы Windows, Linux и их приложения на одном физическом сервере;

– ускорить развитие программного обеспечения и системы тестирования с помощью создания нескольких виртуальных машин на одном сервере;

– упростить поддержку сервера, мониторинг и управление инфраструктурой;

– увеличить коэффициент использования ЦП физического сервера;

– перемещать виртуальные машины с одного физического сервера на другой без изменения конфигурации;

– сохранять состояние виртуальной машины и откатывать конфигурацию к этому состоянию одним щелчком мыши.

Подготовка виртуальной машины

Традиционный центр обработки данных (ЦОД) представляет собой большое количество серверов, размещенных на одной площадке с целью повышения эффективности и защищенности. Защита ЦОД подразумевает сетевую и физическую защиту (а также надежное электропитание). Физическая безопасность – наиболее простая составляющая. Важно обеспечить строгий контроль физического доступа администраторов к серверам и сетевой инфраструктуре. Что касается сетевой защиты, то в первую очередь она подразумевает построение надежной защиты периметра, включающей в себя межсетевой экран, защиту от вторжений. Кроме собственно функций защиты, межсетевой экран используется для сегментирования внутренней сети ЦОД с разделением на подсети с разным уровнем доверия (серверы, доступные из Интернета, серверы, доступные только из внутренней сети компании, и т. д.) [5].

Обновления ОС

WSUS (Windows Software Update Service) – это служба обновления операционных систем Windows 2000/XP/2003, а также других продуктов Microsoft. Эта служба представляет собой локальное зеркало сайта Windows Update. WSUS поддерживает каскадирование (вы можете обновлять

сервер WSUS не только с Windows Update, но и с другого WSUS сервера). Основные обновления направлены на исправление ошибок и потенциальных уязвимостей системы.

Пользуясь сервисом, вы всегда имеете актуальную систему. Как правило, заплатки выходят за несколько недель до появления действующего эксплойта и червя. Таким образом, постоянно обновляемая система становится неуязвимой для абсолютного большинства сетевых червей, размножающихся через ошибки в операционных системах Windows. Снимается угроза эпидемий таких червей как Blaster и Sasser, приводящих к неработоспособности многих узлов сети, нарушению работы Интернета и ухудшению работы сети в целом.

Сетевая структура

Для построения системы потребовалось 3 УЦ (корневой, промежуточный и выдающий УЦ), 1 сервер для синхронизации с сервером из Интернета, 1 сервер для тестирования обновлений и с этим же сервером производят синхронизацию все серверы корпоративной сети (раздаёт обновления). Отдельный сервер понадобится для сканирования систем на вредоносные программы. Поскольку все эти серверы являются гостевыми и находятся в разных сетях, необходимо настроить между ними таблицу маршрутизации, чтобы они могли взаимодействовать между собой. Здесь приводится общая схема автоматизированной системы с указанием ip-адресов серверов и основных шлюзов и построена матрица доступа.

Маршрутизация АС

IP-маршрутизация – процесс выбора пути для передачи пакета в сети. Под путем (маршрутом) понимается последовательность маршрутизаторов, через которые проходит пакет по пути к узлу-назначению. IP-маршрутизатор – это специальное устройство, предназначенное для объединения сетей и обеспечивающее определение пути прохождения пакетов в составной сети. Маршрутизатор должен иметь несколько IP-адресов с номерами сетей, соответствующими номерам объединяемых сетей.

В работе понадобилось настраивать таблицу маршрутизации, поскольку серверы обновлений, сканирования и серверы УЦ находились в разных сетях, для этого, как уже описывалось выше, воспользовались командой route из консоли cmd.exe. Для того чтобы маршрутизация заработала, необходимо включить службу «маршрутизации и удаленного доступа». На рис. 2 представлена реализованная схема виртуальных серверов, которые размещаются на физическом сервере. В неё вошли серверы, которые были использованы в иерархической модели для реализации АС. Чёрными стрелками обозначены обращения между серверами. Пунктирными стрелками обозначены взаимодействия сервера сканирования Trend Micro и внутренних серверов. На рис. 3 представлена схема, на которой реализована практическая часть сетевой модели.

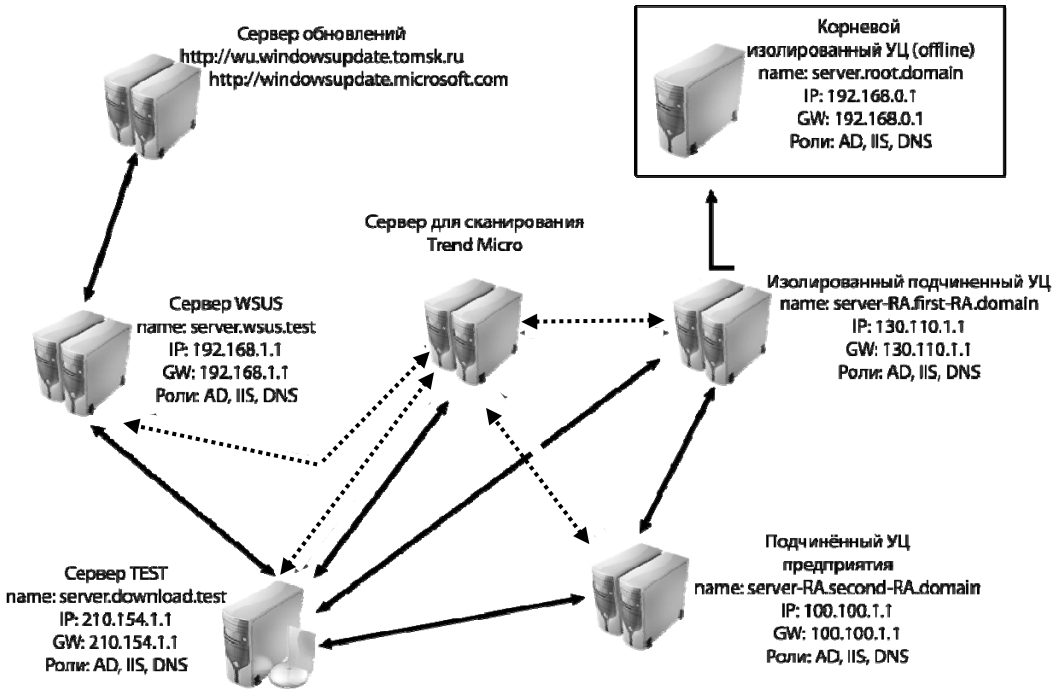

Рис. 2. Реализованная схема виртуальных серверов

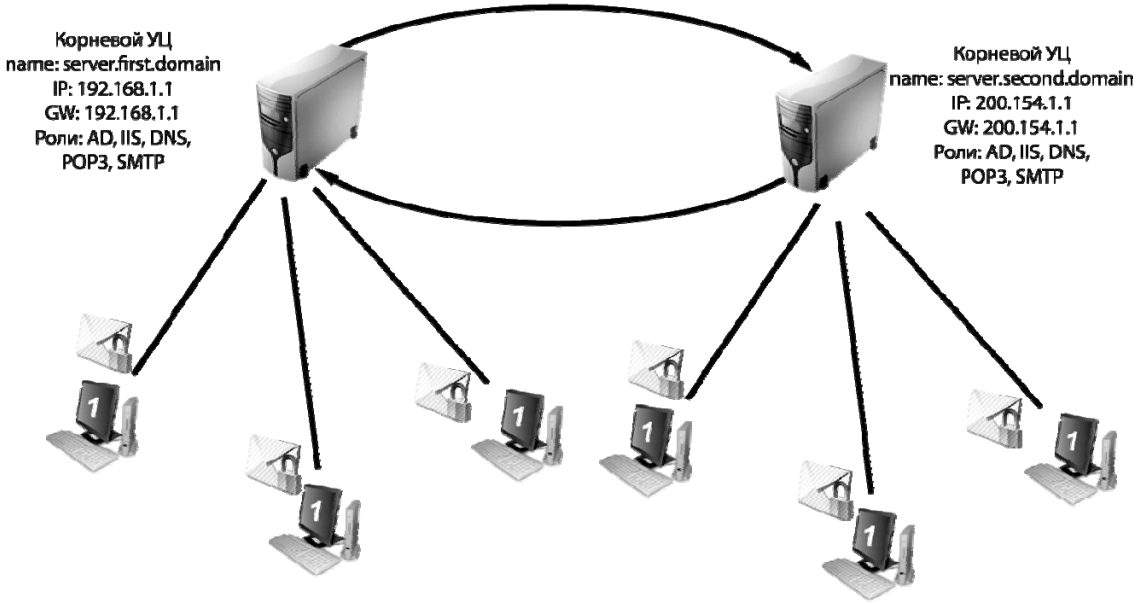

Рис. 3. Схема сетевой модели

Построение матрицы доступа

В реализованной системе используется множество субъектов и объектов:

1) Объекты:
   O1 – сервер обновлений Microsoft;
   O2 – WSUS;
   O3 – сервер теста обновлений (Test Server);
   O4 – корневой УЦ (CA 1);
   O5 – промежуточный УЦ (CA 2);
   O6 – выдающий УЦ (CA 3).
2) Субъекты:
   S1 – WSUS;
   S2 – сервер теста обновлений (Test Server);
   S3 – сканирование (Trend Micro);
   S4 – корневой УЦ (CA 1 – изолированный корневой УЦ);
   S5 – промежуточный УЦ (CA 2 – изолированный подчинённый УЦ);
   S6 – выдающий УЦ (CA 3 – корпоративный подчинённый УЦ);
   S7 – администратор;
   S8 – пользователи.

Отношения субъектов к объектам (право на доступ) представлены в табл. 8.

Таблица 8

Матрица доступа субъектов к объектам

Субъекты/Объекты		Сервер обновлений Microsoft	WSUS	Test Server	Trend Micro	CA 1	CA 2	CA 3
	O/S	O1	O2	O3	O4	O5	O6	O7
WSUS	S1	d		d				
Test Server	S2		d	d	d		d	d
Trend Micro	S3		d	d	d		d	d
CA 1	S4							
CA 2	S5					d		
CA 3	S6						d	
Admin	S7		d	d	d			d
User	S8							d

Примечание: d – доступ субъекта к объекту.

Политика безопасности системы устанавливает такой порядок работы, при котором:

1) WSUS имеет доступ на скачивание обновлений с сервера обновлений Microsoft;

2) сервер теста обновлений имеет доступ на скачивание обновлений с WSUS и в случае успеха позволит синхронизироваться остальным компьютерам корпоративной сети с собой;

3) сервер сканирования серверов имеет доступ ко всем серверам сети организации за исключением CA 1;

4) корневой изолированный УЦ находится offline и не имеет доступа к другим серверам, так же как и они к нему;

5) CA 2 может иметь доступ к CA 1;

6) CA 3 имеет доступ к CA 2;

7) администратор имеет доступ к WSUS, Test Server и Trend Micro, а также CA 3;

8) пользователи имеют доступ только к CA 3.

Заключение

Технологии виртуализации коренным образом меняют подход к развертыванию ИТ-инфраструктуры. Несмотря на все очевидные достоинства виртуализации, ее внедрение рождает множество существенных проблем, описанных выше. Безусловно, эти проблемы могут быть решены при грамотном подходе. Ключевой элемент данного подхода – тщательное планирование всех этапов внедрения виртуализации. На каждом из этапов может потребоваться применение специализированного программного обеспечения, которое не всегда предоставляется производителями платформ бесплатно. По статистике большинство крупных проектов виртуализации закончились неудачей во многом из-за того, что в данный момент сложно оценить их эффективность в количественных показателях, а также отсутствуют средства для сопровождения платформ виртуализации на всех этапах жизненного цикла.

На этапе планирования необходимо уделять особое внимание стратегиям резервного копирования и восстановления после сбоев, учитывать лицензионные требования производителей операционных систем и особенности интеграции с существующей инфраструктурой. Стоит учесть, что технологии виртуализации, с одной стороны, упрощают управление компьютерными системами, с другой – значительно усложняют их структуру. Это рождает необходимость в высококвалифицированных специалистах, которых в данный момент очень мало (хотя, безусловно, их количество будет стремительно расти в связи с востребованностью технологии). Виртуализация уже сейчас используется нефтяными, финансовыми, телекоммуникационными и другими компаниями, являясь незаменимым элементом их ИТ-инфраструктуры. Но полноценного эффекта от виртуализации можно достичь только за счет полного осознания своих потребностей в ней, учета ее требований и тщательнейшего планирования виртуализационного проекта.

Изначально СЭД проектировались без учета применения ЭЦП, они моделировали работу с бумажными документами, от которых организации не собирались отказываться. По мере осознания того, что ЭЦП использовать нужно, разработчики стали встраивать в существующие СЭД функции ЭЦП, рассматривая их как дополнительные. Однако в результате получались решения с ограниченными возможностями, поскольку полноценное встраивание ЭЦП требовало слишком больших переделок в существующих системах.

Сегодня на очередном витке развития информационных технологий разработчики вновь создаваемых СЭД уже не рассматривают ЭЦП как некое дополнение и учитывают необходимость ее применения уже на этапе разработки архитектуры систем, в том числе распределенных [6].

Мировой опыт развития СЭД показывает, что перспективы применения ЭЦП в электронном документообороте и смежных областях весьма впечатляющи. Наблюдается бурное развитие технологий потокового сканирования и распознавания графических образов, что позволяет перевести практически любые бумажные документы в электронный вид и обеспечить эффективный полнотекстовый поиск по ним. Развивается ИОК. В сочетании с общей тенденцией к ускорению принятия решений по документам и потребностью именно в юридически значимых электронных документах это приводит к тому, что электронная цифровая подпись становится востребованной как никогда ранее.

Литература

1. Немного истории. Сравнительный анализ эмуляторов [Электронный ресурс]. – Режим доступа: http://www.xakep.ru/magazine/xs/048/080/1.asp, свободный (дата посещения: 17.11.2011).

2. О виртуальных машинах и гостевых операционных системах. [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ru-ru/library/cc794868(WS.10).aspx, свободный (дата посещения: 17.11.2011).

3. Microsoft Special Interest Group «Neva». [Электронный ресурс]. – Режим доступа: http://www.ci.ru/inform13_01/p17ms.htm, свободный (дата посещения: 17.11.2011).

4. Доверительные отношения между центрами сертификации CA в Windows Server 2003 PKI. [Электронный ресурс]. – Режим доступа: http://www.osp.ru/win2000/2006/07/3546159/, свободный (дата посещения: 17.11.2011).

5. Отчету «2008 Data Breach Investigations Report». [Электронный ресурс]. – Режим доступа: http://securityblog.verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/, свободный (дата посещения: 17.11.2011).

6. Мещеряков Р.В. Распределенный удостоверяющий центр / Р.В. Мещеряков, А.А. Шелупанов // Методы и технические средства обеспечения безопасности информации: матер. конф. Санкт-Петербург, 26–27 ноября 2003 г. – СПб.: Изд-во СПбГПУ, 2003. – 129 с. – С. 61.

Сопов Максим Алексеевич
Ст. преподаватель каф. КИБЭВС ТУСУРа
Тел.: 8 (383-2) 41-34-26
Эл. почта: sma@keva.tusur.ru

Тимченко Сергей Викторович
Д-р физ.-мат. наук, профессор, зав. каф. прикладной математики и информатики ТУСУРа
Эл. почта: tsv@ftf.tsu.ru

Кручинин Виктор Владимирович
Д-р техн. наук, профессор каф. промышленной электроники ТУСУРа
Тел.: (382-2) 51-05-30
Эл. почта: kru@ie.tusur.ru

Чуркин Максим Васильевич
Инженер каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: 8 (383-2) 41-34-26
Эл. почта: time_100@mail.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе ТУСУРа
Тел.: (382-2) 51-05-30
Эл. почта: saa@keva.tusur.ru

Sopov M.A., Timchenko S.V., Kruchinin V.V., Churkin M.V., Shelupanov A.A.

Secure information technology platform of certification authority virtual server

We propose a model of the server identity centers on the basis of information technology platform. We show the efficiency of this configuration with a simultaneous increase in reliability.

Keywords: certification authority, electronic signature, operating model, virtual server.