11 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.9

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЕРТИФИКАТОВ И ПРОТОКОЛОВ SSL/TLS ДЛЯ ШИФРОВАНИЯ ДАННЫХ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

М.Я. Беккер, А.О. Терентьев, Ю.А. Гатчин, Н.С. Кармановский

Рассмотрен вопрос использования цифровых сертификатов и протоколов шифрования данных SSL/TLS в системах облачных вычислений. Показаны основные способы использования цифровых сертификатов для шифрования сетевых соединений, дан анализ особенностей использования этих способов. Предложен подход к решению вопроса о выборе наиболее подходящего способа в условиях различных видов систем облачных вычислений.

Ключевые слова: облачные вычисления, безопасность облачных вычислений, цифровой сертификат, шифрование, SSL, TLS, PKI.

Введение

При переходе к использованию облачных вычислений возникают значительные риски [1], которые требуют совершенствования системы защиты информации с учетом используемого вида облачных служб. При этом одним из первостепенных встает вопрос о защите данных, передаваемых между пользователем и поставщиком услуг [2]. Наиболее распространенным решением этой задачи является использование цифровых сертификатов шифрования и протоколов SSL (Secured Socket Layer) / TLS (Transport Layer Security).

Крупнейшие компании – от поставщиков услуг облачных вычислений (например, социальная сеть Facebook [3]) до производителей аппаратуры (например, SONY [4]) – внедряют функции SSL/TLS шифрования в свои продукты.

Протокол SSL, позволяющий использовать шифрование с открытым ключом для аутентификации и шифрования клиент-серверных соединений, получил широкое распространение во Всемирной сети [5]. Основанный на нем протокол TLS принят Internet Engineering Task Force (IETF) в качестве стандарта RFC-2246 [6], а в 2006 г. обновлен до версии 1.1 (RFC-4346 [7]). Протоколы SSL/TLS позволяют осуществить установление шифрованного соединения с использованием цифрового сертификата сервера и (или) клиента.

Целью настоящей работы является выработка рекомендаций по повышению безопасности передачи данных при проектировании систем облачных вычислений путем использования цифровых сертификатов для шифрования сетевых соединений на базе протоколов SSL/TLS.

Выпуск, хранение, проверка и отзыв цифровых сертификатов

Под цифровым (или электронным) сертификатом шифрования подразумевается электронный документ, содержащий открытый ключ шифрования, а также некоторый набор атрибутов, принадлежащих владельцу ключа. Сертификат может быть не подписан вообще (unsigned), подписан самим владельцем открытого ключа (self-signed, «самоподписной» сертификат) или подписан специальным удостоверяющим центром.

Для безопасного установления зашифрованных сетевых соединений клиент и сервер должны иметь возможность убедиться в достоверности используемых открытых ключей. Однако безопасный прямой обмен сертификатами возможен далеко не всегда. В таком случае клиент и сервер осуществляют проверку при посредстве так называемых удостоверяющих центров (УЦ) или центров сертификации (CA, Certificate Authority).

Систему, обеспечивающую проверку достоверности сертификатов клиентов и серверов при посредстве УЦ, называют инфраструктурой открытых ключей (PKI, Public Key Infrastructure). PKI включает в себя соответствующие аппаратные и программные средства, персонал, регламентные процедуры, необходимые для выпуска, управления, распространения, проверки достоверности и отзыва цифровых сертификатов. УЦ подтверждают достоверность открытого ключа и атрибутов его владельца путем выпуска сертификата, подписанного цифровой подписью удостоверяющего центра.

С целью разработки стандартов PKI, используемых в сети Интернет, в рамках IETF создана соответствующая рабочая группа – PKIX Working Group [8]. Стандартом X.509 определены форматы данных сертификатов и списков отзыва сертификатов, согласно RFC-5280 [9] определен формат сертификатов X.509 версии 3 и списков отзыва сертификатов (CRL, Certificate Revocation List) версии 2.

Для использования цифровых сертификатов каждый клиент и сервер должны располагать индивидуальным локальным хранилищем сертификатов (CS, Certificate store), которое представляет собой упорядоченный набор файлов или базу данных, содержащую сертификаты.

В хранилище располагается, как минимум, набор тех сертификатов, которым доверяет данная система. В том случае, если PKI не используется, достаточно разместить в хранилище неподписанные или «самоподписные» сертификаты доверенных узлов, зарегистрировав их как заслуживающие доверия (trusted).

Также в хранилище могут находиться собственные сертификаты данной системы, которые автоматически или с разрешения пользователя предъявляются при установлении сетевых соединений. Функции хранилища сертификатов могут быть предоставлены для приложений операционной системой либо реализованы в каждом отдельном приложении – web-браузере, web-сервере, почтовом клиенте и т.д. В последнем случае каждое приложение будет иметь собственный набор сертификатов.

При использовании PKI в хранилище также размещаются сертификаты центров сертификации, которым доверяет данная система. Такие сертификаты называются корневыми (RC, Root Certificate), так как они используются при проверке других сертификатов и списков отзыва с учетом установленной сертификационной политики (Certificate Policy, CP – см. RFC-3647 [10]).

С корневого сертификата начинается так называемый «путь проверки» (certificate validation path), который может включать несколько промежуточных звеньев. Путь проверки может быть построен через различные последовательности сертификатов от различных удостоверяющих центров. Этот процесс называют поиском пути (path discovery). Выбор пути проверки может осуществляться проверяющим клиентом самостоятельно (например, с помощью CryptoAPI, появившегося в операционных системах Windows, начиная с Windows NT 4.0 [11]). Также поиск пути может быть делегирован специальному серверу в соответствии с предложенным для этой цели протоколом SVCP согласно RFC-5055 [12].

Помимо самих сертификатов, центры сертификации могут использовать списки отзыва сертификатов (CRL), представляющие собой списки отозванных сертификатов с указанием времени отзыва, подписанные удостоверяющим центром. Такие списки свободно распространяются через общедоступный сетевой ресурс. При проверке сертификата с помощью PKI проверяющая система проверяет не только подпись сертификата и срок его действия, но также отсутствие его в соответствующем списке отзыва.

Количество отозванных сертификатов крупных PKI может быть довольно значительным, что вызывает рост накладных расходов при их проверке клиентом. Для решения этой проблемы разработан протокол проверки статуса отзыва сертификата в режиме «online» (OCSP, Online Certificate Status Protocol), принятый в качестве стандарта RFC-2560 [13]. Сервер OCSP распространяет информацию о статусе сертификатов в виде так называемых доказательств (proofs), защищенных с помощью электронной цифровой подписи, в виде ответов на запрос в соответствии с протоколом OCSP или в виде сокращенных списков отозванных сертификатов (MiniCLR). В сертификате, выпущенном в рамках соответствующей PKI, может быть указан адрес сервера OCSP для проверки статуса отзыва данного сертификата.

Следует обратить внимание, что при проверке срока действия сертификата используется текущая системная дата и время. Некорректная установка системной даты и времени является одной из наиболее распространенных проблем при использовании цифровых сертификатов. Для предотвращения возникновения таких проблем рекомендуется использовать системы сетевой синхронизации даты и времени с соответствующими серверами.

Таким образом, цифровые сертификаты в системах облачных вычислений могут применяться различными способами, в зависимости от используемой инфраструктуры, экономических показателей, требований, предъявляемых к системе обеспечения безопасности.

Шифрование передаваемых данных с использованием SSL/TLS

Чаще всего в качестве основного атрибута сертификата сервера используется доменное имя. При проверке сертификата сервера клиент имеет возможность убедиться, что он осуществляет сеанс связи (сессию) именно с сервером владельца данного доменного имени. Также важнейшим атрибутом любого сертификата является срок годности, устанавливающий календарную дату окончания его срока действия. В качестве прочих атрибутов клиентского сертификата чаще всего используются персональные данные физического лица – пользователя облачных служб (фамилия, имя, отчество, дата рождения, адрес, номер лицевого счета, адрес электронной почты и т.д.).

После успешной проверки достоверности сертификатов они могут быть использованы не только для шифрования передаваемых данных, но также для аутентификации и авторизации [14].

Однако аутентификация и авторизация с использованием цифровых сертификатов требует отдельного рассмотрения и выходит за рамки настоящей работы. Отметим только, что, как правило, цифровые сертификаты используют не в качестве основного средства, а в качестве компонента многофакторной системы аутентификации/авторизации, в особенности в гетерогенных информационных системах с использованием облачных вычислений. При этом применение сертификатов для аутентификации клиентов имеет особую важность для отклонения запросов от клиентов, не обладающих привилегиями доступа к службам, но маскирующихся под них (например, отклонения попыток доступа с использованием украденной аутентифицирующей информации другого вида, такой как имя пользователя и пароль).

Далее будем рассматривать использование протоколов SSL/TLS для шифрования передаваемых данных. Шифрование передаваемых данных обеспечивает защиту от прослушивания сетевых соединений и атак типа man-in-the-middle, при которых злоумышленник внедряется в цепочку сетевого соединения в качестве одного из промежуточных узлов.

Очевидно, что для защиты от перечисленных угроз достаточно проверить достоверность сертификата только с одной стороны, после чего ключ шифрования сессии может быть передан безопасным способом. В этой связи при использовании SSL/TLS в системах облачных вычислений чаще всего ограничиваются проверкой сертификата сервера, что упрощает администрирование и снижает эксплуатационные издержки клиентов, поскольку системы клиент–сервер подразумевают незначительное количество серверов, обслуживающих значительное количество клиентов.

Основным программным обеспечением пользователя систем облачных вычислений является web-браузер. Все популярные на сегодняшний день web-браузеры поддерживают протокол HTTPS (HTTP Secured), принятый в качестве стандарта RFC-2818 [15]. Сам по себе протокол HTTPS не является самостоятельным протоколом, а представляет собой режим использования SSL/TLS протоколов для шифрования HTTP-соединения, установленного по протоколу TCP.

Таким образом, наиболее распространенным и экономически обоснованным подходом к шифрованию сетевых соединений в системах облачных вычислений является SSL/TLS шифрование с использованием сертификатов, предъявляемых со стороны сервера при установлении такого соединения. Однако при этом предстоит решить вопрос о том, каким способом осуществляется выпуск, распространение и проверка сертификатов, что и будет далее рассмотрено.

Использование PKI сторонних поставщиков

В работе [1] авторами подробно рассмотрен вопрос классификации систем облачных вычислений по видам пользовательской аудитории (или так называемой «области видимости»), где два вида таких систем можно выделить как основные – это публичные (общего пользования) и частные (с кругом пользователей, как правило, ограниченным контрагентами или сотрудниками одной организации).

Для публичных облачных систем существует сеть PKI общего пользования, которая используется по умолчанию всеми распространенными web-браузерами. В комплект поставки современного web-браузера входит набор сертификатов широко известных общедоступных центров сертификации, которые производитель браузера считает достойными доверия. Подобные наборы сертификатов также обычно входят в комплект поставки различного программного обеспечения, такого как операционные системы, серверы сетевых служб и т.д.

Сеть PKI общего пользования используется публичными облачными службами. Как правило, заключение договора на обслуживание, а также оплата услуг платных служб происходит в начале использования такой службы через сеть Интернет, причем потребитель услуг и поставщик могут находиться в противоположных точках земного шара. Очевидно, что в этом случае сложно предложить альтернативу использованию PKI общего пользования от одного из известных общедоступных сертификационных центров.

Такие центры сертификации предлагают организациям и частным лицам услуги по выпуску и обслуживанию цифровых сертификатов, как правило, на платной основе. Выпущенный ими сертификат может быть проверен практически любым пользователем или сервером в сети Интернет, поскольку сертификат такого центра с большой вероятностью уже присутствует в хранилище соответствующего узла, установленный вместе с операционной системой или соответствующим клиентским или серверным программным обеспечением (ПО).

Кроме того, услуги некоторых сертификационных центров, сертификаты которых входят в комплект поставки большинства современных web-браузеров, можно получить и бесплатно [16].

Выпускаемые центрами сертификации сертификаты могут иметь различные уровни доверия. При подключении по протоколу HTTPS большинство web-браузеров не только отображают в адресной строке наименование протокола «https://...», но и сообщают пользователю уровень доверия к используемому сертификату и дополнительную информацию о нем (например, выделяют адресную строку цветом в соответствии с уровнем доверия к предъявленному web-сервером сертификату, причем высокий уровень доверия обозначается зеленым цветом, а более низкий – синим, показывают краткое наименование центра выдачи сертификата, и т.д.).

Таким образом, использование PKI сторонних поставщиков оправдано при развертывании публичных облачных служб, пользователем которых может стать любой желающий при наличии подключения к сети Интернет.

В частном облаке можно использовать сеть PKI сторонних поставщиков точно так же, как это осуществляется при использовании публичных облачных служб. Во многих случаях при разработке политики безопасности использование пользователями web-браузера с набором корневых сертификатов, поставляемого в комплекте с операционной системой, и приобретение для серверов предприятия сертификата одного из центров сертификации, которому доверяет поставщик операционной системы, может быть признано достаточным для установления защищенных соединений.

Однако использование PKI сторонних поставщиков влечет за собой все риски, характерные для использования облачных вычислений вообще и подробно рассмотренные авторами в работе [1]. Особенно следует обратить внимание на риск потери контроля, поскольку отзыв сертификата в этом случае возможен только при посредстве поставщика услуг. Более того, необходимо учитывать, что доверить стороннему поставщику приходится не просто одну из используемых сетевых служб, а сетевую службу, являющуюся основой обеспечения безопасности всех остальных используемых служб.

Также следует учитывать, что при использовании набора корневых сертификатов, установленного вместе с программным обеспечением, наличие уязвимости одного из соответствующих центров сертификации компрометирует всю систему. Таким образом, надежность такой системы обеспечения информационной безопасности определяется надежностью самого слабозащищенного центра сертификации, количество которых довольно велико.

С учетом изложенного очевидно, что во многих случаях при разработке политики безопасности предприятия встает вопрос о поиске более безопасного способа использования цифровых сертификатов, чем PKI сторонних поставщиков.

Создание «собственной» PKI

Под «собственной» будем понимать такую инфраструктуру публичных ключей, которая полностью управляется и контролируется специалистами использующей ее организации.

В случае построения частной системы облачных вычислений необходимо определиться, целесообразно ли использование PKI вообще, или же можно ограничиться прямым обменом сертификатами. Вполне вероятно, что в ряде случаев вполне возможно обойтись без PKI, выпустив необходимые сертификаты и установив их непосредственно в хранилище клиентских и серверных систем вручную или при помощи административного программного обеспечения. Использование же PKI при наличии разветвленной компьютерной сети со значительным количеством серверов и пользователей имеет преимущество с точки зрения обеспечения безопасности, которое заключается в возможности гибкого управления подчиненными сертификатами и их сроками действия. При наличии PKI администратор может в любое время объявить любой из ранее выпущенных сертификатов недействительным при помощи списка отзыва сертификатов (CRL), что значительно повышает степень защиты информации.

При создании «собственной» PKI-инфраструктуры выделяются, как правило, соответствующие ресурсы для ее первоначального создания и дальнейшей поддержки. Поскольку необходимо обеспечить как выпуск, так и проверку сертификатов, одним из основных требований к подобной инфраструктуре является высокий уровень ее работоспособности (способность обслуживать большое количество запросов проверки, отказоустойчивость, возможность быстрого восстановления после аварий и т.д.). Кроме того, службы проверки сертификатов должны быть топологически доступны для сетевых запросов соответствующих клиентов и серверов.

Администратор узла PKI может при помощи управления PKI выпустить новый сертификат или объявить существующий недействительным, что значительно повысит степень защиты информации и гибкость управления этой защитой, но будет предъявлять более жесткие требования к информационной безопасности самих узлов PKI.

Самой простой вариант организации PKI – система с одиночным узлом УЦ. В этом случае все клиенты имеют в хранилище доверенный сертификат этого единственного одиночного узла.

Для организации, имеющей более одного крупного подразделения, система с одиночным узлом может оказаться недостаточно гибкой. Тогда обычно используют иерархическую PKI. В этом случае все клиенты доверяют одному головному УЦ, но в системе существуют другие УЦ, которые подчиняются вышестоящему УЦ вплоть до головного, образуя древовидную структуру. Это позволяет делегировать полномочия по выпуску сертификатов отдельных групп пользователей и серверов на более низкие уровни, гибко реагировать на возможные проблемы информационной безопасности в одной из «ветвей», обслуживающей, например, одно из подразделений организации, не затрагивая всю остальную систему.

В случае доверительных отношений между держателями отдельных УЦ возможно построение сетевой PKI, когда некоторые УЦ непосредственно доверяют другим УЦ без посредничества головного центра, а клиенты доверяют только «своему» УЦ.

На практике же чаще всего встречаются смешанные варианты перечисленных выше архитектур, могущие порождать очень сложные цепочки сертификации. Для лучшего контроля над ситуацией часто используется строго иерархическая структура в рамках организации, но при этом выделяется отдельный УЦ, называемый мостовым, который отвечает за доверительные взаимоотношения с УЦ других организаций.

Таким образом, выбор структуры «собственной» PKI осуществляется, в первую очередь, в зависимости от структуры организации, а также ее взаимоотношений с другими организациями – контрагентами.

Одновременное использование нескольких наборов сертификатов или PKI

Как показано в работе [1], на сегодняшний день редко можно встретить публичные и частные облачные системы в чистом виде. На практике, как правило, возникает необходимость одновременного

использования ресурсов предприятия и публичных облачных служб. Следует обратить внимание, что при использовании собственных сертификатов или развертывании «собственной» PKI простое добавление выпущенных сертификатов в общее хранилище сертификатов пользовательских систем и приложений, например web-браузера, может оказаться недостаточным для обеспечения должного уровня защиты. Дело в том, что при этом web-браузер признает доверенными как добавленные сертификаты, так и предустановленные ранее корневые сертификаты. Следовательно, при уязвимости одного из центров сертификации она может быть использована для атаки на корпоративные ресурсы частного облака, так как поддельный сертификат будет признан достоверным при обращении к корпоративным ресурсам. В то же время удаление предустановленных корневых сертификатов также не приведет к желаемому результату, так как пользователь лишается возможности использования защищенных HTTPS-соединений с публичными службами в штатном режиме.

Задача обеспечения высокого уровня информационной безопасности в случае одновременного использования публичных облачных служб и защиты с помощью собственных сертификатов может быть решена различными способами.

Решение этой задачи возможно на стороне клиента. Например, можно использовать разные хранилища для корневых сертификатов PKI общего пользования и собственных сертификатов. Для этого используется дополнительное специализированное программное обеспечение, поскольку в настоящее время в распространенных web-браузерах отсутствует возможность настройки хранилища для использования разных наборов сертификатов при работе в различных сетевых зонах. Авторами направлено предложение производителям ведущих web-браузеров о добавлении такой функции в будущих версиях, что позволит осуществлять более тонкую настройку клиентских систем и во многих случаях избавит администраторов от необходимости использования дополнительного программного обеспечения.

Решение рассматриваемой задачи возможно также средствами сервера при использовании «собственной» PKI. В этом случае клиентское ПО настраивается на использование только «собственной» PKI, из хранилища клиентов удаляются прочие предустановленные сертификаты (при их наличии), а проверка сертификатов публичных облачных служб осуществляется при посредстве «собственной» PKI.

Рекомендации разработчикам систем безопасности облачных вычислений

Приведенный выше сравнительный анализ позволяет сформулировать следующие рекомендации разработчикам систем безопасности облачных вычислений по выбору способа использования цифровых сертификатов для шифрования данных.

- Для систем с невысокими требованиями к гибкости смены сертификатов при высокой критичности уровня затрат, а также для тестовых и пилотных систем рекомендуется использование «самоподписных» сертификатов и их прямая установка на пользовательские и серверные узлы.
- Для систем с высокими требованиями к уровню защиты информации и топологически гарантированными сетевыми соединениями клиентов облачных служб с инфраструктурой организации-поставщика служб рекомендуется использование «собственной» PKI инфраструктуры.
- Для публичных облачных служб, а также систем с требованиями к защите информации, допускающими использование субподрядчиков, имеющих гарантированные сетевые соединения клиентов облачных служб с сетевыми ресурсами проверки сертификатов (как правило, через сеть Интернет) рекомендуется приобретение сертификатов соответствующих доверенных поставщиков.

Выбор способа использования сертификатов должен начинаться с максимально точной количественной оценки приоритетов – уровня защищенности информации, степени риска, срока жизни решения, уровня первоначальных затрат, стоимости поддержки решения, стоимости перехода от одного способа к другому и т.п.

При выборе способа использования сертификатов следует предусмотреть и оценить возможные варианты перехода в будущем на альтернативные способы (в частности, если система критериев выбора изменится со временем). При этом наиболее затратным является использование «собственной» PKI организации, дающей возможность обеспечения максимальной степени защиты информации.

Заключение

Использование шифрования на базе протоколов SSL/TLS в системах облачных вычислений влечет за собой необходимость обеспечить выпуск, распространение и проверку цифровых сертификатов, как минимум, с одной стороны сетевого соединения.

Авторами проведен анализ и выявлены особенности трех основных способов использования цифровых сертификатов поставщиками и пользователями систем облачных вычислений: использование PKI сторонних поставщиков, разработка и внедрение «собственной» PKI, прямой обмен сертификатами. Предложен подход к выбору способа использования цифровых сертификатов при облачных вычислениях с учетом особенностей каждого способа.

Наиболее безопасным способом использования цифровых сертификатов является создание «собственной» PKI. Однако этот способ требует значительных затрат. Одновременное использование не-

скольких наборов сертификатов или PKI позволяет обеспечить требуемый уровень безопасности для каждой используемой сетевой зоны.

Выработаны рекомендации разработчикам систем безопасности облачных вычислений, использующих цифровые сертификаты для шифрования сетевых соединений на базе протоколов SSL/TLS, которые позволяют минимизировать риски и оптимизировать экономические показатели с учетом вида проектируемых и эксплуатируемых облачных служб.

Литература

1. Беккер М.Я., Гатчин Ю.А., Кармановский Н.С., Терентьев А.О., Федоров Д.Ю. Информационная безопасность при облачных вычислениях: проблемы и перспективы // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 1(71). – С. 97–102.
2. Sicherheitsrisiken der Cloud sind beherrschbar. Virtualisierungs guide [Электронный ресурс]. – Режим доступа: http://www.virtualisierungs-guide.de/Sicherheit/tabid/267/articleType/ArticleView/articleId/13535/Sicherheitsrisiken-der-Cloud-sind-beherrschbar.aspx, свободный. Яз. нем. (дата обращения 12.05.2011).
3. Facebook nun mit durchgehender SSL-Verschlüsselung. Der Standard [Электронный ресурс]. – Режим доступа: http://derstandard.at/1295570976708/Facebook-nun-mit-durchgehender-SSL-Verschluesselung, свободный. Яз. нем. (дата обращения 12.05.2011).
4. Kein Trickraub mit Netzwerkkameras. SONY [Электронный ресурс]. – Режим доступа: http://www.sony.de/biz/content/id/1189437949068/section/produkt/product/nvmfixedcameras?preserveContext=true, свободный. Яз. нем. (дата обращения 12.05.2011).
5. Introduction to SSL. Mozilla Developer Network [Электронный ресурс]. – Режим доступа: https://developer.mozilla.org/en/Introduction_to_SSL, свободный. Яз. англ. (дата обращения 12.05.2011).
6. The TLS Protocol Version 1.0. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://datatracker.ietf.org/doc/rfc2246/, свободный. Яз. англ. (дата обращения 12.05.2011).
7. The Transport Layer Security (TLS) Protocol Version 1.1. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://datatracker.ietf.org/doc/rfc4346/, свободный. Яз. англ. (дата обращения 12.05.2011).
8. PKIX Working Group. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://datatracker.ietf.org/wg/pkix/charter/, свободный. Яз. англ. (дата обращения 12.05.2011).
9. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc5280, свободный. Яз. англ. (дата обращения 12.05.2011).
10. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc3647, свободный. Яз. англ. (дата обращения 12.05.2011).
11. Poking Around Under the Hood: A Programmer's View of Windows NT 4.0. Microsoft Developer Network [Электронный ресурс]. – Режим доступа: http://www.microsoft.com/msj/archive/S413.aspx, свободный. Яз. англ. (дата обращения 12.05.2011).
12. Server-Based Certificate Validation Protocol. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc5055, свободный. Яз. англ. (дата обращения 12.05.2011).
13. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc2560, свободный. Яз. англ. (дата обращения 12.05.2011).
14. An Internet Attribute Certificate Profile for Authorization. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc5755, свободный. Яз. англ. (дата обращения 12.05.2011).
15. HTTP Over TLS. The Internet Engineering Task Force [Электронный ресурс]. – Режим доступа: http://datatracker.ietf.org/doc/rfc2818/, свободный. Яз. англ. (дата обращения 12.05.2011).
16. StartSSL Free. StartSSL [Электронный ресурс]. – Режим доступа: http://www.startssl.com/?app=1, свободный. Яз. англ. (дата обращения 12.05.2011).

Беккер Михаил Яковлевич – Microsoft Deutschland GmbH, ведущий консультант, mbecker@microsoft.com

Терентьев Андрей Олегович – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, аспирант, 9444828@mail.ru

Гатчин Юрий Арменакович – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор технических наук, профессор, зав. кафедрой, gatchin@mail.ifmo.ru

Кармановский Николай Сергеевич – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, кандидат технических наук, доцент, karmanov50@mail.ru