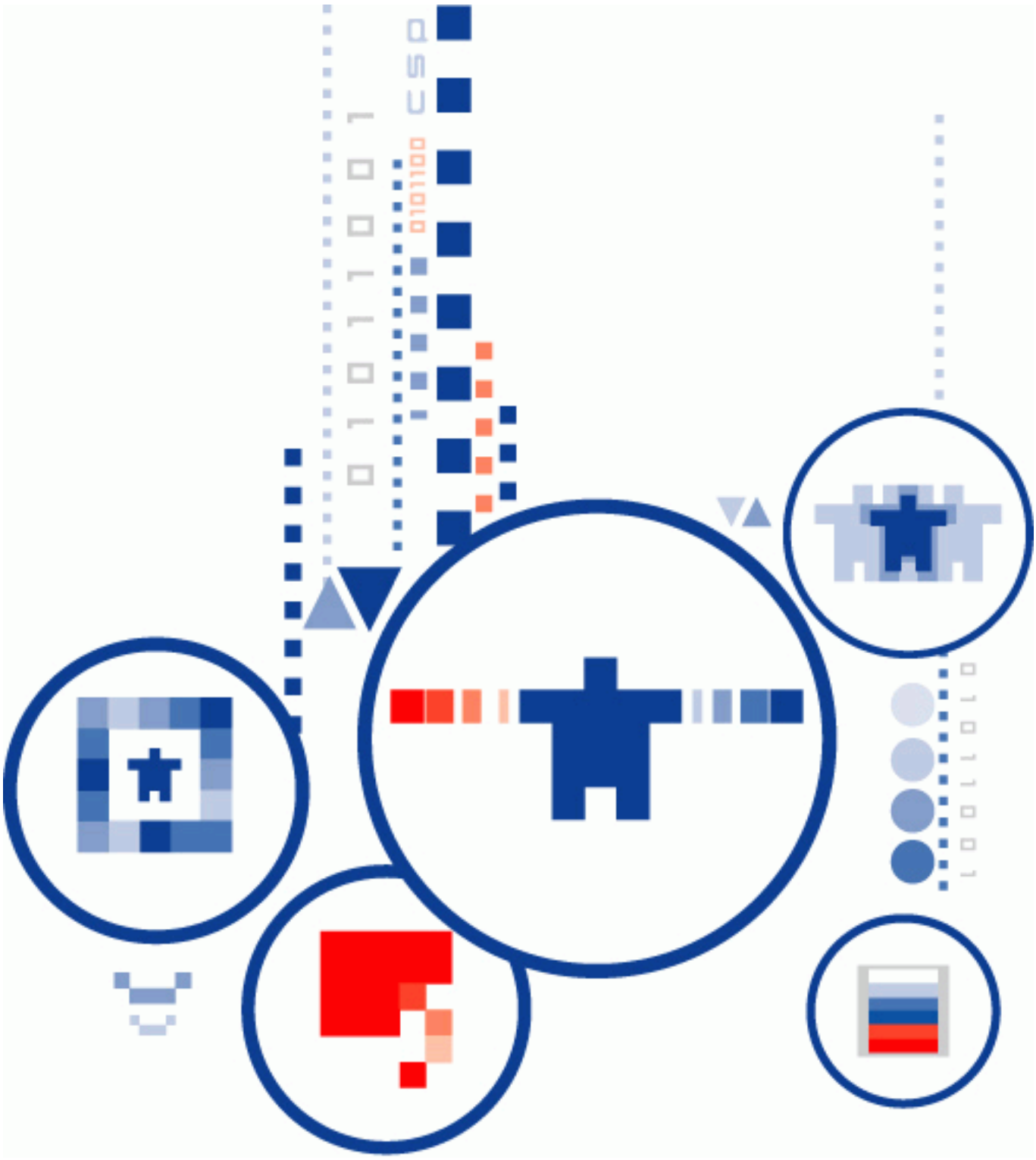
УТВЕРЖДЁН
ЖТЯИ.00023-01 20 01-ЛУ

ЖТЯИ.00023-01 90 04



Использование КриптоПро OCSP Server совместно с КриптоПро УЦ

АННОТАЦИЯ

Настоящий документ содержит описание вариантов совместного использования продуктов КриптоПро OCSP Server и КриптоПро УЦ для предоставления пользователям актуальной информации о статусах сертификатов по протоколу OCSP.

Рассматриваются варианты использования в качестве источника информации о статусах сертификатов баз данных Центра Сертификации и Центра Регистрации, а также резервирования этих источников с помощью списков отзыва сертификатов (COC).

Описывается способ организации доступа пользователей к OCSP-серверам, обеспечивающий отказоустойчивость.

Приводится сравнение различных методов предоставления информации о статусах сертификатов пользователям.

Информация о разработчике ПК «КриптоПро OCSP Server» и «КриптоПро УЦ»:

ООО «Крипто-Про»

127018, г. Москва, ул. Сущевский вал, д. 16, стр.5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

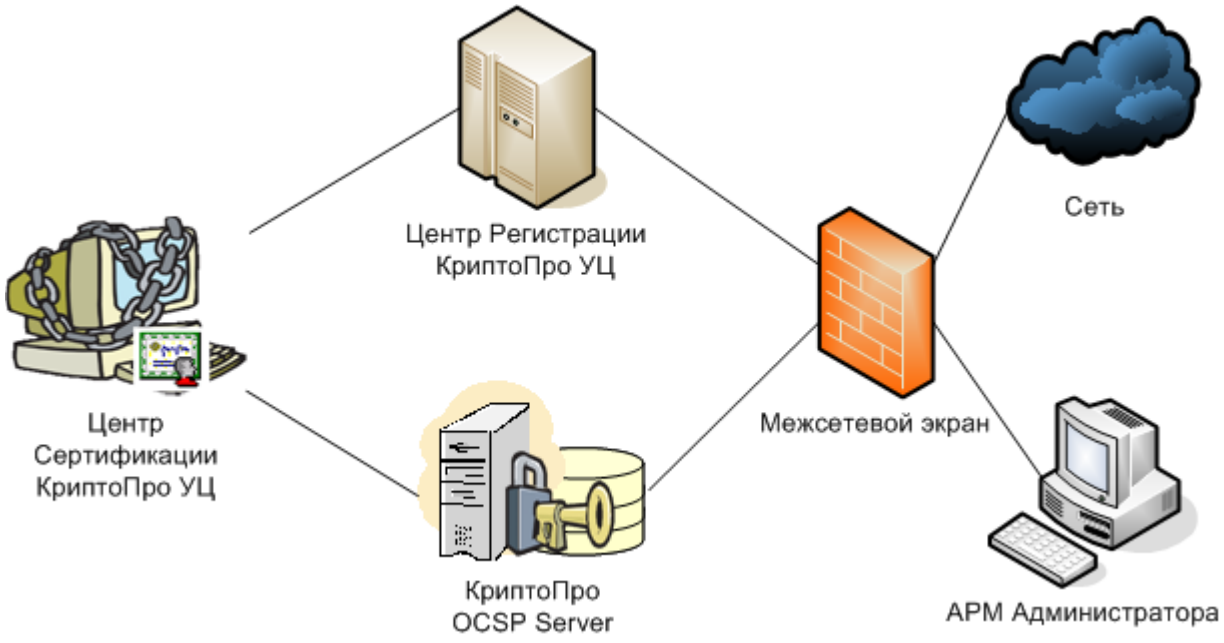
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Типовая схема взаимодействия

На рисунке (см. Рисунок 1) представлена типовая схема взаимодействия компонент КриптоПро УЦ и КриптоПро OCSP Server.

Рисунок 1. Типовая схема взаимодействия компонент КриптоПро УЦ и КриптоПро OCSP Server



Предлагаемая схема соответствует типовой схеме размещения и взаимодействия компонент УЦ в сети предприятия, приведённой в разделе 4.3 документа [OCSPADM]. К схеме взаимодействия компонент УЦ добавлен КриптоПро OCSP Server на отдельном компьютере, подключенный к межсетевому экрану и Центру Сертификации.

Источниками информации о статусах сертификатов для КриптоПро OCSP Server могут являться:

- База данных Центра Сертификации.
- База данных Центра Регистрации.
- Списки отзыва сертификатов.

Для работы по БД Центра Сертификации необходимо выполнить настройку OCSP Server и ЦС в соответствии с разделом 6.1 документа «КриптоПро OCSP Server. Руководство администратора». При этом защита ЦС на сетевом уровне может быть выполнена одним из следующих способов:

- На компьютере ЦС настроить встроенный в ОС персональный межсетевой экран с целью оставить открытыми только необходимые порты, а именно порты для протоколов HTTP, HTTPS (для ЦР) и RPC (для OCSP Server).
- На компьютер ЦС установить межсетевой экран Microsoft ISA Server 2004, в котором настроить для соединений с OCSP Server фильтр приложений RPC (Application filter) в соответствии с Руководством администратора КриптоПро OCSP Server.

Для работы по БД Центра Регистрации необходимо выполнить настройку OCSP Server и ЦР в соответствии с разделом 6.3 документа [OCSPADM]. При этом защита ЦР на сетевом уровне обеспечивается настройкой межсетевого экрана, обозначенного на схеме. Настраивается фильтрация соединений от OCSP Server к ЦР, разрешающая только сетевое взаимодействие, необходимое для доступа к серверу MSDE.

Для работы по СОС необходимо настроить их автоматическую публикацию на OCSP Server. Публикация может осуществляться как с ЦС, так и с ЦР. Настройка выполняется следующим образом:

1. Настраивается новая задача переноса СОС с ЦС или ЦР на OCSP Server.
2. На OCSP Server настраивается папка-приёмник, в которую задача переноса будет помещать СОС по протоколу HTTP.

В последующих двух разделах описаны схемы взаимодействия компонент ПК при использовании одного источника информации о статусах сертификатов. Следует отметить, что помимо представленных в этих разделах схем взаимодействия OCSP Server с УЦ для получения информации из баз данных ЦС или ЦР возможны и любые гибридные схемы подключения. В каждом конкретном случае схема строится, исходя из нужд обеспечения доступности услуг УЦ и OCSP Server для пользователей, в том числе и для отказоустойчивости.

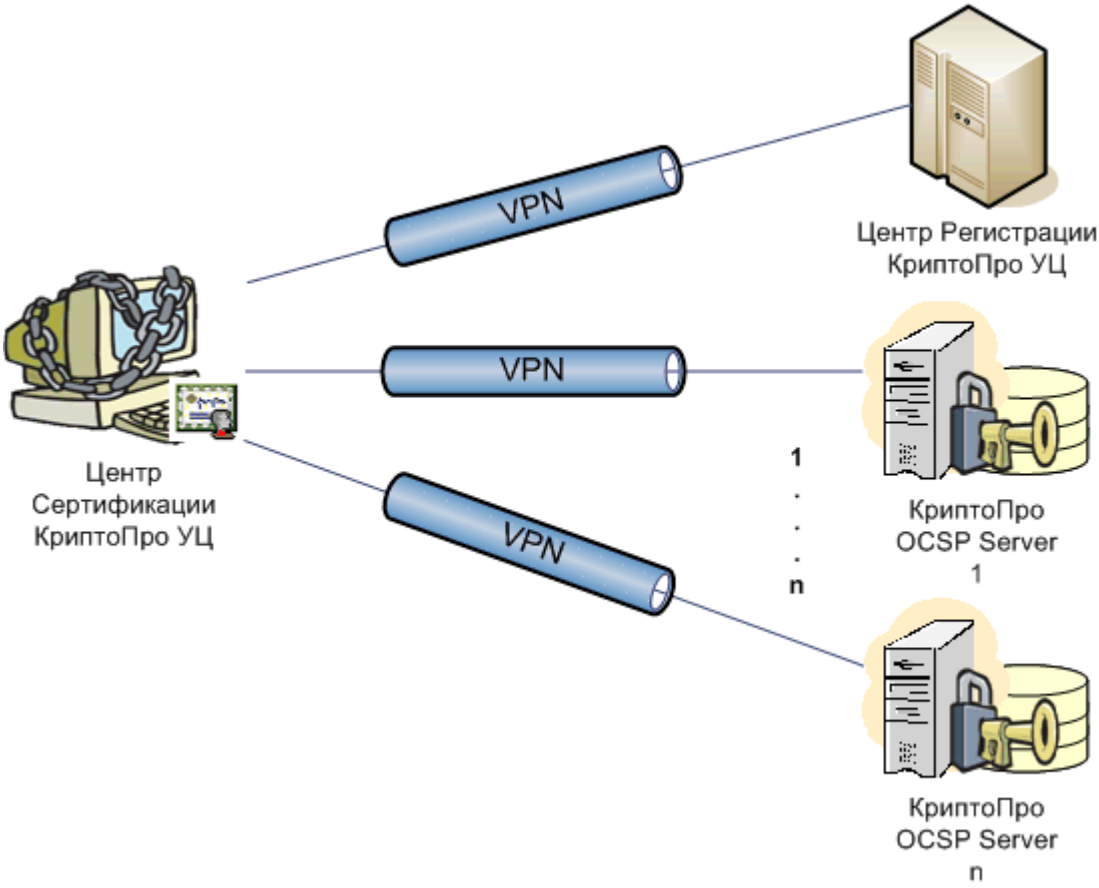
2. Работа по базе данных Центра Сертификации

Данный режим обеспечивает наибольшую актуальность информации в OCSP-ответах, поскольку работа идёт непосредственно с базой данных, хранящей информацию о статусах сертификатов.

При расположении аппаратного обеспечения УЦ и OCSP Server на одной площадке схема соединений компонент соответствует типовой (см. Рисунок 1).

Для обеспечения отказоустойчивости повышения качества оказываемых услуг и для других целей аппаратные компоненты УЦ и OCSP Server могут располагаться на разных площадках. На рисунке (см. Рисунок 2) представлена схема взаимодействия компонент УЦ и OCSP Server для работы по БД Центра Сертификации при размещении на разных площадках. Эта схема разработана на более абстрактном уровне, чем типовая схема взаимодействия.

Рисунок 2. Схема взаимодействия компонент УЦ и OCSP Server для работы по БД Центра Сертификации при размещении на разных площадках



В данной схеме сетевые взаимодействия между ЦС и OCSP Server точно такие же, как и в типовой схеме, только поверх VPN.

Для обеспечения отказоустойчивости возможна установка нескольких OCSP Server на разных площадках и резервирование с использованием COC в качестве источника информации о статусах сертификатов при недоступности ЦС.

Если на компьютере с ЦС КриптоПро УЦ установлен КриптоПро Revocation Provider, а КриптоПро OCSP Server работает по базе данных ЦС, то при выпуске сертификата возникает ошибка из-за особенностей работы службы сертификации Microsoft. Служба сертификации Microsoft сразу после подписания сертификата, но до его занесения в БД ЦС проверяет статус выдаваемого сертификата, что приводит к обращению к OCSP-серверу, который, в свою очередь, обращается к БД ЦС, в которую сертификат еще не занесён. Таким образом, OCSP-сервер вернет ответ со статусом **unknown** и сертификат не будет выдан как не прошедший проверку.

В этом случае удалите КриптоПро Revocation Provider с компьютера ЦС, или запретите ему обращаться к данному OCSP-серверу, указав его адрес в групповой политике **Службы OCSP: запрещенные службы OCSP**.

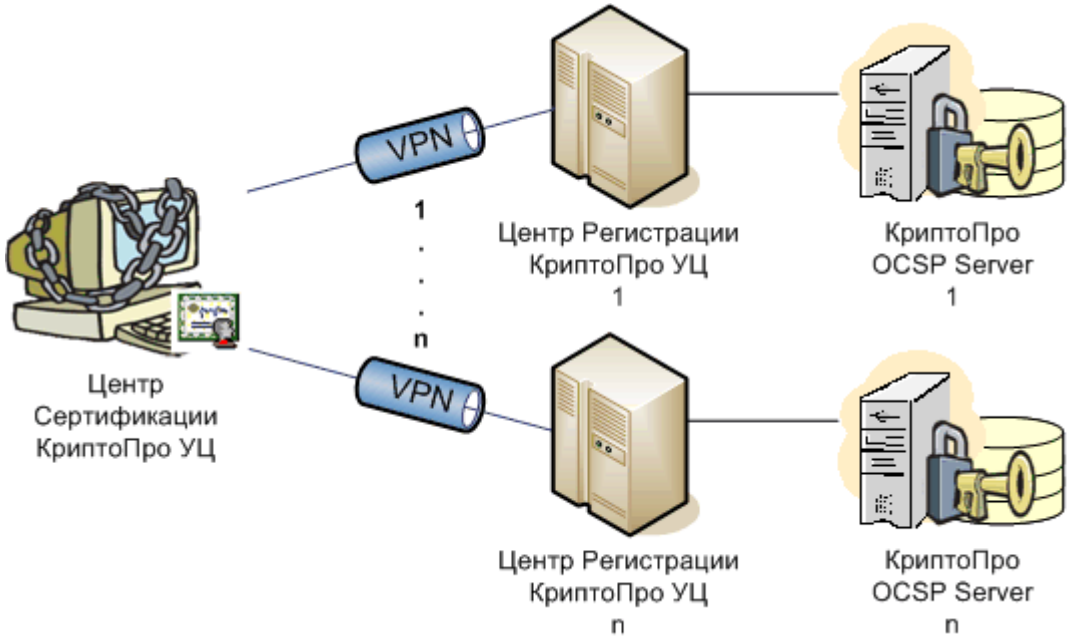
3. Работа по базе данных Центра Регистрации

Данный режим обеспечивает высокую актуальность информации в OCSP-ответах, оставляя возможность работы с отключением ЦС.

При расположении аппаратного обеспечения УЦ и OCSP Server на одной площадке схема соединений компонент соответствует типовой (см. Рисунок 1), за исключением того, что при получении COC только с ЦР отсутствует необходимость прямого соединения ЦС и OCSP Server.

На рисунке (см. Рисунок 3) представлена схема взаимодействия компонент УЦ и OCSP Server для работы по БД Центра Регистрации при размещении на разных площадках. Эта схема разработана на более абстрактном уровне, чем типовая схема взаимодействия.

Рисунок 3. Схема взаимодействия компонент УЦ и OCSP Server для работы по БД Центра Регистрации при размещении на разных площадках



В данной схеме сетевые взаимодействия между ЦР и OCSP Server точно такие же, как и в типовой схеме.

Для обеспечения отказоустойчивости возможна установка нескольких OCSP Server рядом с каждым Центром Регистрации и резервирование с использованием COC в качестве источника информации о статусах сертификатов при недоступности ЦР.

Если на компьютере с ЦС КриптоПро УЦ установлен КриптоПро Revocation Provider, а КриптоПро OCSP Server работает по базе данных ЦР, то при проведении ряда операций с УЦ могут возникнуть взаимные блокировки. Блокировки возможны, если при проведении транзакции возникает необходимость в проверке статуса какого-либо сертификата. Такая проверка приводит к обращению к OCSP-серверу, который, в свою очередь, обращается к таблицам БД ЦР. Но в данный момент выполняется транзакция, и нужные таблицы будут заблокированы до её окончания.

В этом случае удалите КриптоПро Revocation Provider с компьютера ЦС, или запретите ему обращаться к данному OCSP-серверу, указав его адрес в групповой политике **Службы OCSP: запрещенные службы OCSP**.

4. Указание адресов OCSP для обеспечения отказоустойчивости

В данном разделе предлагается способ организации доступа к OCSP-серверам в территориально распределенной системе с большим числом пользователей, обеспечивающий отказоустойчивое обслуживание. Данный способ может применяться в этих же целях в любых других информационных системах, с небольшими модификациями, учитывающими особенности этих систем.

Поскольку клиенты определяют местоположение OCSP-серверов по точке AIA в сертификате, предлагается включать в сертификаты две точки AIA в следующем порядке:

1. Локальный адрес.
2. Глобальный адрес.

Под локальными и глобальными адресами здесь подразумевается использование DNS-имен, которые будут разрешаться в IP-адреса следующим образом. В локальном адресе будет содержаться имя сервера, подобное **local.ocsp.myis.ru**, а в глобальном – **global.ocsp.myis.ru**. При этом DNS-серверы распределенной системы настраиваются таким образом, что имя **global.ocsp.myis.ru** имеет одинаковые IP-адреса для всех пользователей и ссылается на центральный OCSP-сервер – максимально надежный, а имя **local.ocsp.myis.ru** имеет разные IP-адреса для разных пользователей, тем самым обеспечивая обращение пользователя к ближайшему OCSP-серверу. Для ещё большего повышения отказоустойчивости можно развернуть на каждой площадке несколько OCSP-серверов, работающих в режиме балансировки нагрузки между ними.

Подобную настройку DNS можно осуществить, например, одним из следующих способов:

- Создать зону ocsp.myis.ru на всех DNS-серверах системы как первичную и настроить два указанных имени на каждом сервере. local.ocsp.myis.ru – на ближайший(е) сервер(ы), global.ocsp.myis.ru – на центральный(е) сервер(ы). В этом случае управление адресами будет распределенным.
- Сопоставить два указанных имени с множеством всех адресов серверов распространения COC. global.ocsp.myis.ru – один или несколько центральных серверов, local.ocsp.myis.ru – все региональные серверы. Такую настройку необходимо осуществить на первичном DNS-сервере системы, с которого адреса будут автоматически получены всеми вторичными серверами. При запросе адреса сервера local.ocsp.myis.ru служба DNS в ответе упорядочит все известные ей адреса по принципу близости к подсети клиента, таким образом, первый адрес будет указывать на ближайший сервер. Возможность такого автоматического упорядочивания на основе адреса подсети клиента присутствует в наиболее распространенных продуктах – службе DNS в ОС Microsoft и BIND в ОС UNIX. В этом случае управление адресами будет централизованным.

Указанный порядок точек AIA в сертификате обеспечивает следующую логику работы приложений. Первая попытка получения COC происходит на территориально ближайший сервер. Если по каким-либо причинам попытка неудачна, то второе обращение происходит к центральному серверу.

Подробнее о балансировке нагрузки и обеспечении отказоустойчивости доступа пользователей к информации о статусах сертификатов см. в [PKILB].

5. Сравнение методов предоставления информации о статусах сертификатов

В таблице (см. Таблица 1) представлены сравнительные характеристики различных методов предоставления информации о статусах сертификатов пользователям. Сравнение проводится по следующим параметрам:

- необходимость установки дополнительного ПО или изменения существующего,
- актуальность информации о статусах сертификатов,
- отказоустойчивость.

Таблица 1. Сравнение методов предоставления информации о статусах сертификатов

№ п/п	Метод предоставления информации	Установка дополнительного ПО	Модификация существующего ПО	Актуальность	Отказоустойчивость	
					Одна точка CDP или AIA	Две точки CDP или AIA
1	COC	Не требуется	Не требуется	Максимальная задержка равна периоду публикации COC	Не обеспечивает	Обеспечивает, кроме отказов УЦ
2	COC + CRLUpdate	Установка CRLUpdate	Встраивание вызова CRLUpdate	Лучше п. 1 при внеочередных публикациях COC	Не обеспечивает	Обеспечивает, кроме отказов УЦ
3	OCSP-сервер, работающий по COC	Установка КриптоПро Revocation Provider	Не требуется	Соответствует п. 2	Обеспечивает, кроме отказов самого OCSP-сервера	Обеспечивает
4	OCSP-сервер, работающий по БД ЦС с резервированием по COC	Установка КриптоПро Revocation Provider	Не требуется	Наибольшая актуальность информации	Обеспечивает, кроме отказов самого OCSP-сервера	Обеспечивает
5	OCSP-сервер, работающий по БД ЦР с резервированием по COC	Установка КриптоПро Revocation Provider	Не требуется	Наибольшая актуальность информации для сертификатов «своего» ЦР, для других соответствует п. 1	Обеспечивает, кроме отказов самого OCSP-сервера	Обеспечивает

6. Перечень сокращений

AIA	Точка доступа к информации о Центре (Authority Information Access)
CDP	Точка доступа к СОС (CRL Distribution Point)
DNS	Доменная система имён (Domain Name System)
HTTP	Протокол передачи гипертекста (Hypertext Transfer Protocol)
HTTPS	Безопасный протокол передачи гипертекста (Secure HTTPS)
IP	Протокол Интернет (Internet Protocol)
OCSP	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
RPC	Удалённый вызов процедур (Remote Procedure Call)
VPN	Виртуальная частная сеть (Virtual Private Network)
АРМ	Автоматизированное рабочее место
БД	База данных
ОС	Операционная система
ПК	Программный комплекс
СОС	Список отзыва сертификатов (CRL – Certificate Revocation List)
УЦ	Удостоверяющий Центр
ЦР	Центр Регистрации
ЦС	Центр Сертификации

7. Перечень рисунков

8. Перечень ссылочных документов

[OCSPADM] ЖТЯИ.00023-01 90 01. “КриптоПро OCSP Server. Руководство администратора”.

[PKILB] Смирнов П. Балансировка нагрузки и отказоустойчивость при проверке статусов сертификатов в ИОК // PCWEEK Russian Edition, №44(458), 2004. – с. 24-26.
http://kis.pcweek.ru/Year2004/N44/CP1251/NetWeek/chapt3.htm