УДК 004.056

М.А. Сопов, А.Ю. Крайнов, А.А. Шелупанов

Модели повышения уровня информационной безопасности удостоверяющего центра

Предложены модели повышения уровня информационной безопасности распределенных удостоверяющих центров, основанные на параллельной работе, дублировании и резервировании систем. Определены и обоснованы критерии, влияющие на уровень информационной безопасности функционирования удостоверяющих центров.

Ключевые слова: удостоверяющий центр, электронная подпись, модель функционирования.

Модели функционирования удостоверяющего центра

Развитие электронного документооборота, различных Internet-сервисов привело к необходимости внедрения и совершенствования методов их защиты. Обеспечение электронному документу целостности, однозначная идентификация человека, написавшего электронный документ или использовавшего Internet-сервис, обеспечение конфиденциальности и невозможности человеку, не обладающему определенными правами прочитать документ или проследить сервис, – это те компоненты обеспечения защиты, которые необходимо обеспечивать. Решением описанных проблем стало применение шифрования и электронной подписи (ЭП). Разработанные на основе инфраструктуры открытых ключей (ИОК или PKI) методы защиты доказали на практике свою жизнеспособность и эффективность.

Основным инструментом, реализующим инфраструктуру открытых ключей, является удостоверяющий центр.

Развитие удостоверяющих центров, обслуживающих органы государственной власти, коммерческие и корпоративные проекты, повлекло за собой развитие распределенных комплексов удостоверяющих центров. Необходимость таких структур осознает и Министерство связи и массовых коммуникаций, создавая и совершенствуя под своей эгидой второй проект по упорядочиванию и регулированию деятельности данных комплексов. Рассматривая данные комплексы с точки зрения разных проектов, можно выделить разные факторы, которые влияют на организацию работы этих комплексов, но в общем итоге и для государственных, и для коммерческих проектов удостоверяющих центров необходима надежно функционирующая структура.

Классическая модель функционирования удостоверяющего центра

Два основных компонента удостоверяющего центра (УЦ) – это центр регистрации (ЦР) и центр сертификации (ЦС) (рис. 1). ЦР-компонент обеспечивает регистрацию пользователей в базе данных и формирование запросов ЦС на изготовление сертификатов. ЦС ведет базу данных сертификатов и изготавливает сертификаты открытых ключей. Данные компоненты связаны между собой по защищенному каналу связи. С клиентами взаимодействует только ЦР, данные каналы могут быть открытыми и защищаться межсетевыми экранами и сканерами безопасности.

Как показала десятилетняя практика, при создании распределенных структур УЦ эффективнее использовать иерархические структуры, которые не образуют «колец», возможных при мостовых, сетевых или гибридных структурах. Но с учетом того, что как для коммерческих, так и для государственных структур необходима эффективная работа УЦ, то соответственно необходимо из данных моделей функционирования исключить угрозы, связанные с нарушением функционирования данных моделей.

Для исключения угроз нарушения функционирования необходимо повысить уровень защищенности структуры за счет повышения ее надежности. Для реализации распределенных моделей УЦ с учетом повышения их защищенности можно выделить следующие схемы повышения надежности:

– параллельная работа;

– дублирование;

– резервирование.

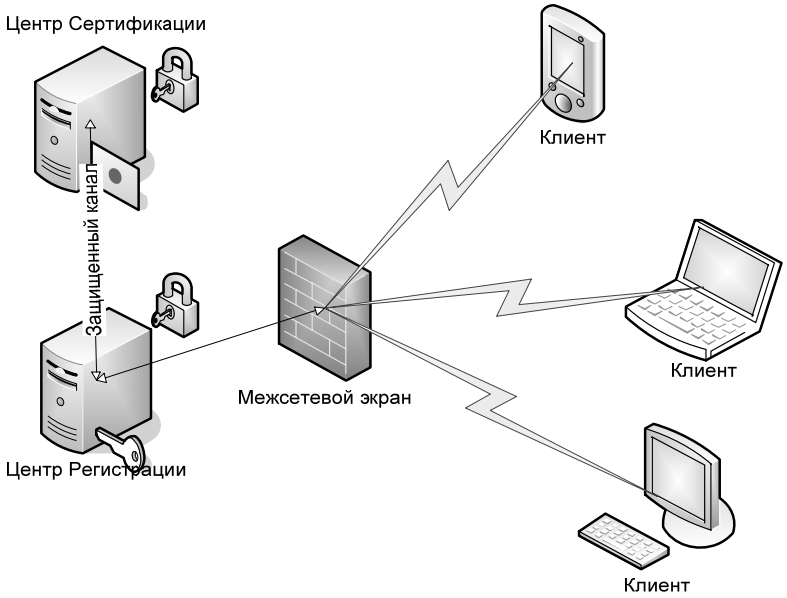

Рис. 1. Модель функционирования УЦ

Модели повышения уровня информационной безопасности УЦ

Модель параллельной работы распределенной структуры УЦ (рис. 2) подразумевает создание в одной области по крайней мере двух УЦ одного уровня, работающих независимо друг от друга. Данные УЦ должны обладать одинаковыми правилами резервирования аппаратуры, архивирования и хранения данных, а также согласованных регламентных мероприятий по взаимодействию между ними, предполагающих координацию действий по развертыванию регистрационных центров на уровне компетентностного подхода, а также отлаженного четкого механизма взаимодействия. Использование данной схемы снижает нагрузку на систему УЦ, распределяя ее между несколькими равносильными УЦ.

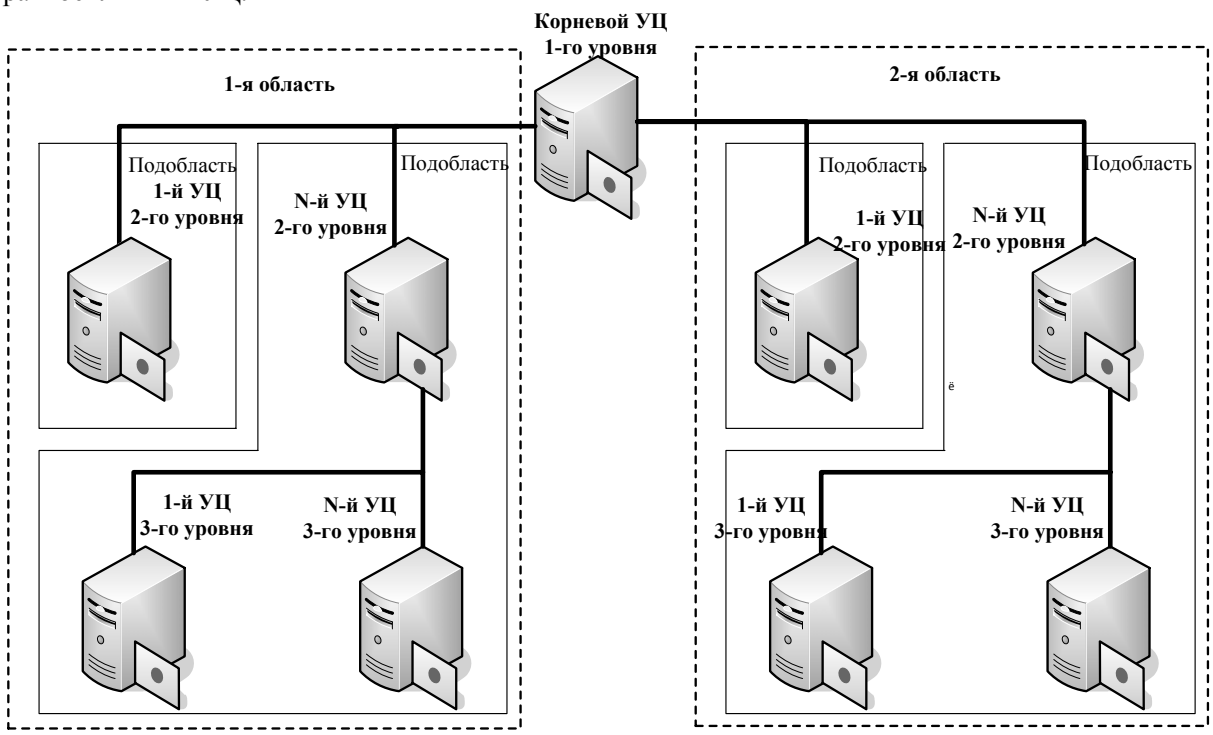

Рис. 2. Модель параллельной работы распределенной структуры УЦ

Дублирование – параллельная работа удостоверяющих центров независимо друг от друга в одной области (рис. 3). При использовании такой модели должна осуществляться синхронизация баз

данных сертификатов (желательно по защищенному каналу) по единым правилам резервирования аппаратуры, архивирования и хранения данных.

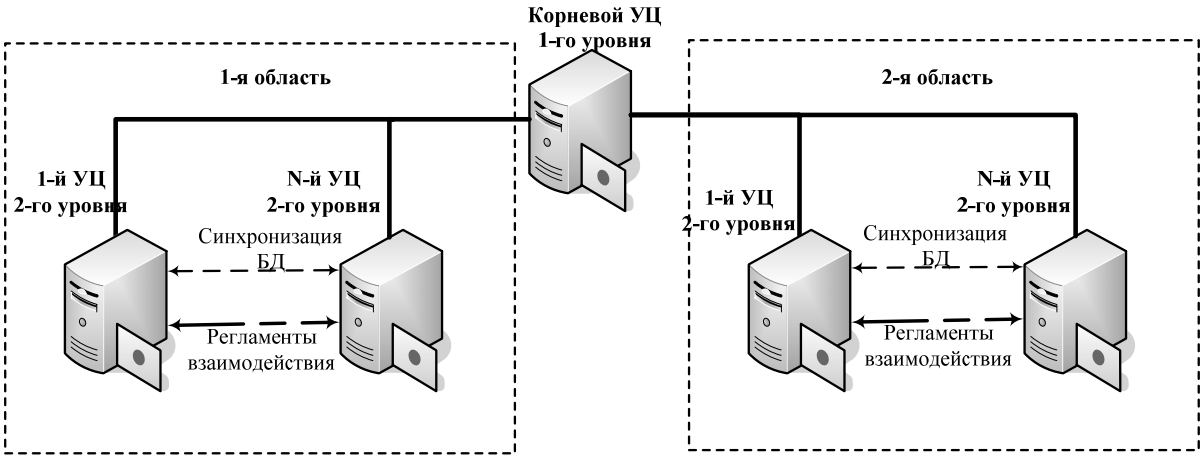

Рис. 3. Модель дублирования распределенной структуры УЦ

Резервирование – создание в области двух УЦ второго уровня с одинаковыми правилами работы резервирования аппаратуры и архивирования и хранения данных (рис. 4). работа ведется основным УЦ, резервный УЦ работает в случае отказа основного.

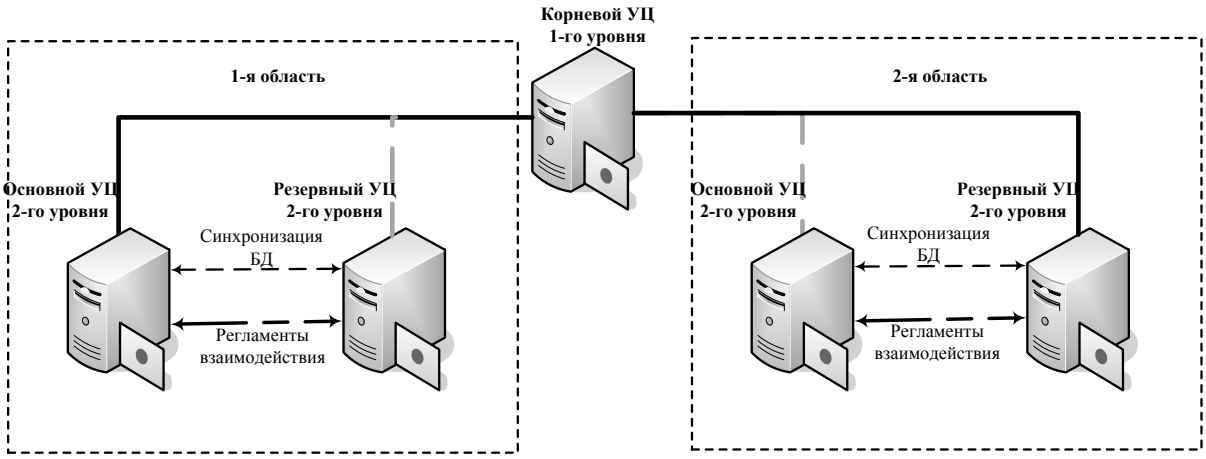

Рис. 4. Модель резервирования распределенной структуры УЦ

Методика повышения уровня информационной безопасности

При анализе систем УЦ с целью определения критериев, оказывающих влияние на уровень информационной безопасности, установлено, что:

– система УЦ – большая сложная система;

– система УЦ имеет сложное описание и большой объем технической документации;

– система УЦ представляет собой совокупность не только аппаратных, но и программных средств, имеющих различные свойства;

– система УЦ – это совокупность элементов для обработки информации, что требует ведения контроля не только за правильностью ее работы, но и за достоверностью обработки информации;

– система УЦ – это объект, работающий при наличии внешних возмущающих факторов: аппаратных, в канале передачи, в канале ввода информации, а также нарушений, связанных с невыполнением регламентных требований.

Основываясь на проведенном анализе, выделены основные критерии:

– оборудование и техника;

– программное обеспечение;

– персонал;

– территориальная распределенность;

– обслуживаемые проекты;

– форс-мажорные обстоятельства.

Оборудование и техника

Основываясь на действующем российском законодательстве, а также на нормативных документах, для использования шифрования и ЭП необходимо сертифицированное оборудование, техника и программное обеспечение.

Тем не менее необходимо рассчитывать надежность функционирования программно-аппаратной платформы системы УЦ.

Используя соотношение (1), можно рассчитать надежность оборудования и техники в комплексе:

$$P_{\text{маш}} = 1 - \sum_{i=m+1}^{m+n} C_{m+n}^{m+n-i} * p^{m+n-i} * (1-p)^{i} . \quad (1)$$

Зная надежность каждого сервера или компьютера, можно получить надежность всего комплекса, где n – это количество серверов или компьютеров, необходимых для работы системы УЦ, а m – это количество серверов или компьютеров, являющихся резервными.

Программное обеспечение

Особенностью ПО является сложность расчета надежности его функционирования. Параметром, характеризующим надежность работы ПО, является время наработки программы на отказ.

Необходимо отметить, что в большинстве случаев надежность работы ПО ограничивается надежностью работы аппаратного обеспечения. Тем не менее надежность функционирования должна обязательно учитываться в критически важных элементах и узлах функционирования системы. При предоставлении разработчиком тестов наработки на отказ, надежности системы расчет можно провести по формуле (1).

Персонал

Человек является самым уязвимым звеном в системе УЦ, так как на него влияет множество внешних и внутренних факторов.

В штате УЦ выделяются критически важные должности:

1) руководитель УЦ;
2) уполномоченное лицо УЦ;
3) администратор по информационной безопасности;
4) администратор УЦ;
5) оператор УЦ;
6) системный администратор.

Ответственность при работе со средствами криптографической защиты информации, оказании услуг органам государственной власти и муниципального управления, оказание услуг участникам электронных торгов и сдачи различной отчетности в электронной форме требует высокой квалификации. В данном случае требования к квалификации определяются, исходя из задач, выполняемых штатной единицей, совокупностью опыта работы и соответствующего образования.

Особым моментом является то, что замещение должностей в случае выхода из строя одного из сотрудников происходит сверху вниз, т.е. старшая должность замещает младшую, за исключением должности системного администратора (рис. 5). Такое условие характеризуется, исходя из объявленных критериев к кандидату на конкретную должность и политики информационной безопасности УЦ: разграничением прав на администрирование телекоммуникационных служб и доступом к различному уровню конфиденциальности информации.

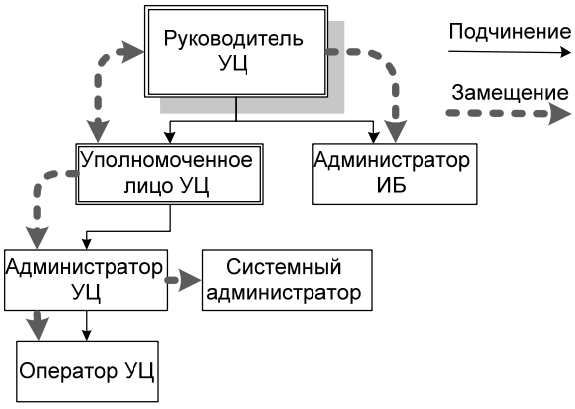

Рис. 5. Замещение должностей УЦ

Важным показателем для работы персонала является количество выпускаемых сертификатов. В зависимости от данного показателя определяется количество персонала, достаточного для выполнения функционала УЦ:

$$K_{\text{cer}} = \frac{n}{365 * K_{\text{cer}}}, \quad (2)$$

где n – общее количество сертификатов за год; K_{cer} – среднее количество сертификатов изготавливаемое за день УЦ, исходя из интенсивности работы УЦ.

Период в 1 календарный год обусловлен двумя факторами:

1) срок действия сертификата;
2) неравномерное распределение выдачи сертификатов в течение года.

Территориальная распределенность

Территориальная распределенность УЦ должна опираться не только на наличие изложенных факторов, т.е. на техническую оснащенность реально действующего УЦ, кадровую политику и научный потенциал, но и на наличие каналов телекоммуникационной связи, территориальную распределенность, т.е. площадь, покрываемую данным УЦ, плотность населения в данном регионе, а также на возможность оперативного решения возникающих проблем на территории региона.

Так как телекоммуникационные каналы связи не относятся (не принадлежат) к УЦ, то ответственность за их функционирование возлагается на провайдера.

Обслуживаемые проекты

Проекты, которые обслуживает УЦ, разделяются на проекты ИОГВ и коммерческие. Наличие каждого вида проекта предъявляет различные требования к условиям и содержанию работы УЦ, временным рамкам, условиям регламентных работ и т.д. Таким образом, ответственность и риски УЦ прямо пропорциональны количеству проектов, выполняемых УЦ.

Форс-мажорные обстоятельства

К форс-мажорным обстоятельствам можно отнести стихийные бедствия и преднамеренные и непреднамеренные человеческие воздействия, которые могут повлечь за собой негативные последствия, например пожар.

При данных обстоятельствах УЦ должен обладать катастрофоустойчивостью и планами продолжения и восстановления бизнеса.

Литература

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – Кн. 1. – 400 с.

2. Ермаков А.В. Электронная цифровая подпись в системе госзакупок / А.В. Ермаков, Е.В. Хухлаев // Открытые системы. – 2002. – № 7–8. – С. 62–68.

3. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. – М.: Вильямс, 2001. – 672 с.

4. Основы информационной безопасности / Р.В. Мещеряков, А.А. Шелупанов, Е.Б. Белов, В.П. Лось. – М.: Горячая линия – Телеком, 2006.– 544 с.

5. Липаев В.В. Надежность программного обеспечения АСУ. – М.: Энергоиздат, 1981. – 240 с.

6. Майерс Г. Надежность программного обеспечения. – М.: Мир, 1980. – 360 с.

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

Крайнов Алексей Юрьевич
Д-р физ.-мат. наук, доцент, зам. декана физико-технического факультета
Национального исследовательского Томского государственного университета
Эл. почта: office@keva.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе
Томского государственного университета систем управления и радиоэлектроники
Тел.: (382-2) 51-05-30
Эл. почта: saa@keva.tusur.ru

Sopov M.A., Krainov A.Yu., Shelupanov A.A.
Models of increasing the information security level of certification authority

In the article we offer the models of increasing security of distributed certification authority, based on parallel operation, duplication and redundancy systems. We defined and proved the criteria which influence the information security level of certification authorities.
Keywords: Certification authority, electronic signature, operating model.