На правах рукописи

Коротаев Никита Васильевич

Методы сравнительного анализа программных средств реализации инфраструктуры открытых ключей в экономических информационных системах

Специальность 08.00.13 – математические и инструментальные методы экономики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата экономических наук

Ростов-на-Дону – 2009

Работа выполнена в ГОУВПО «Ростовский государственный экономический университет (РИНХ)».

Научный руководитель: доктор экономических наук, доцент
Тищенко Евгений Николаевич

Официальные оппоненты: доктор экономических наук
Калиниченко Владимир Иванович

кандидат технических наук, доцент
Долженко Алексей Иванович

Ведущая организация: ГОУВПО «Южно-Российский государственный университет экономики и сервиса»

Защита состоится 22 декабря 2009 года в 11:00 на заседании диссертационного совета ДМ 212.209.03 в Ростовском государственном экономическом университете (РИНХ) по адресу: 344002, г. Ростов-на-Дону, ул. Большая Садовая, 69, ауд. 231.

С диссертацией можно ознакомиться в научной библиотеке Ростовского государственного экономического университета (РИНХ)

Автореферат разослан 20 ноября 2009 года.

Ученый секретарь
диссертационного совета И.Ю. Шполянская

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современное информационное взаимодействие требует высокой скорости передачи данных, что приводит к увеличению доли информационных технологий, используемых в этом взаимодействии. В состав передаваемых данных неизбежно включается все более важная информация (персональные данные, сведения, содержащие коммерческую тайну, и многое другое), которая передается через незащищенную сеть Интернет. Для обеспечения целостности данных, их аутентичности, юридической значимости и невозможности отказа от авторства используется асимметричная криптография, которая легла в основу инфраструктуры открытых ключей (PKI).

Однако бесконтрольное возникновение и стремительное развитие локальных, коммерческих, отраслевых и внутриведомственных PKI-систем привело к формированию разрозненного информационного пространства, где удостоверяющие центры не были связаны доверием между собой. Этим фактом объясняется их многообразие.

В настоящий момент большинство из удостоверяющих центров входит в единый домен доверия, что предоставляет пользователю выбор PKI-системы, соответствующей его предпочтениям. Это делает актуальным вопрос о методах сравнительного анализа PKI-систем с целью нахождения одной, наиболее подходящей пользователю. Главными критериями, которые будут участвовать в процессе отбора, будут качество и полнота предоставляемых услуг, стоимость приобретения и внедрения, трудоемкость выполнения операций и простота использования.

Рассматривая вопрос с другой стороны (с позиции владельца PKI-системы), можно выделить потребность в эффективной организации структуры систем, заинтересованность в полноте и качестве предоставляемых ими услуг с целью привлечения максимального числа пользователей PKI-системы и максимизации прибыли. Так, наряду с методами, применяемыми пользователем,

обладающим меньшим количеством информации и возможностей, здесь необходимо использовать также методы управления структурой PKI-системы.

Обобщая цели двух субъектов, можно говорить о сравнительном анализе характеристик объектов, а именно программных продуктов, на основе которых строится PKI-система. От их функциональных возможностей, быстродействия, стоимости и других свойств будет зависеть результат потребительского выбора.

Степень разработанности проблемы. Вопросам потребительского качества программного обеспечения посвящено множество трудов отечественных и иностранных ученых. В работах таких исследователей, как В.В. Липаев, В.В. Дик, Г.Н. Хубаев, Ф.Г. Гурвич, Г. Майерс, Б. Боэм, Дж. Браун, Х. Каспар и другие, рассмотрены основные понятия, факторы и методы анализа характеристик качества сложных программных средств.

Вопросам разработки и анализа характеристик информационных систем посвящены работы Г.Н. Хубаева, К.Р. Адамадзиева, С.В. Баранова, Г. Буча, К. Дж. Дейта, Е.Н. Тищенко, А. Джекобсона, А.А. Емельянова, Е.Н. Ефимова, С.В. Ивахненкова, Э. Кармайкла, Г. Майерса, Б. Мейера, Э. Нейбурга, Дж. Рамбо, Д. Хейвуда, А. Элиенса и др.

Нам неизвестны исследования, посвященные сравнительному анализу и совершенствованию потребительского качества информационных продуктов, используемых в инфраструктуре открытых ключей. Также нет работ, посвященных выбору оптимальной структуры PKI-систем.

Цель и задачи диссертационного исследования. Целью работы является развитие инструментария сравнительного анализа потребительского качества PKI-систем и разработки методического аппарата для принятия решений при создании, эксплуатации и развитии PKI-инфраструктуры.

Задачи, решаемые в диссертационной работе:

- разработка универсальной модели инфраструктуры PKI-систем;
- разработка и развитие методов сравнительной оценки потребительского качества PKI-систем;

- разработка и развитие методов совершенствования структуры PKI-систем.

Объектом исследования являются экономические информационные системы, используемые организациями и частными лицами, принимающими участие в электронном документообороте, управлении сертификатами, электронной торговле, защищенной электронной почте и других областях, поддерживаемых инфраструктурой открытых ключей.

Предметом исследования являются процессы проектирования и использования программных продуктов, относящихся к инфраструктуре открытых ключей, а также методы анализа их потребительского качества.

Теоретической основой исследования являются научные труды российских и зарубежных ученых по теории выбора и принятия решений, экономико-математическому моделированию. В проведенном исследовании использовались элементы теории информационных систем и статистического анализа. Также использовались вероятностные методы определения качества сложных систем и методы анализа предметной области.

Работа проведена в рамках пункта 2.6 «Развитие теоретических основ, методологии и инструментария проектирования, разработки и сопровождения информационных систем субъектов экономической деятельности: методы формализованного представления предметной области, программные средства, базы данных, корпоративные хранилища данных, базы знаний, коммуникационные технологии» паспорта специальности 08.00.13 – математические и инструментальные методы экономики.

Эмпирической базой исследования явились экспериментальные и статистические данные, собранные в процессе эксплуатации экономических информационных систем ряда организаций, использующих инфраструктуру открытых ключей. Основные выдвигаемые научные положения и рекомендации экспериментально подтверждены. Поставленные эксперименты составляют основу предлагаемой методологии исследования.

Инструментарий исследования составили классические методы анализа защищенности распределенных экономических информационных систем, методы сравнения программных систем по критерию функциональной полноты, методы целочисленного программирования, а также программные средства общего и специального назначения.

Нормативно-правовой базой исследования являются федеральные законы «Об электронной цифровой подписи» от 10.01.2002 г. № 1-ФЗ, «Об информации, информатизации и защите информации» от 20.02.1995 г. № 24-ФЗ (с изменениями от 10.01.2003 г.), ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Положения диссертации, выносимые на защиту:

- перечень функциональных операций, состоящий из 75-ти наименований, разделенный по областям применения, позволяющий сравнивать PKI-системы по критерию функциональной полноты;
- метод расчета трудоемкости выполнения группы функциональных операций в PKI-системе, позволяющий оценивать затраты времени на выполнение группы функциональных операций, а также их транзакций при заданной вероятности;
- профиль PKI-системы, включающий в себя функциональные операции и время их выполнения, позволяющий проводить сравнительный анализ PKI-систем и определять рекомендации по повышению их эффективности.

Научная новизна исследования. Результаты исследования содержат следующие элементы научной новизны:

- составлен перечень функциональных операций (75 операций) для инфраструктуры открытых ключей, отличающийся детализацией элементарных операций до уровня сетевых протоколов и позволяющий сравнивать PKI-системы по критерию функциональной полноты;

- разработан метод расчета трудоемкости выполнения группы функциональных операций в PKI-системе, отличающийся использованием частот обращения к функциональным операциям и рассчитанных статистических характеристик выполнения каждой элементарной операции и позволяющий оценивать затраты времени на выполнение группы функциональных операций и их транзакций при заданной вероятности;
- разработан метод определения эффективного числа узлов в PKI-системе, отличающийся применением модели целочисленного программирования к системе массового обслуживания, построенной на основе программного кластера PKI-системы, и позволяющий путем последовательного перебора для области допустимых решений найти необходимое число узлов в системе для достижения заданной пропускной способности;
- сформирован профиль PKI-системы, включающий в себя перечень функциональных операций и время их выполнения, отличающийся использованием вероятностно-временных характеристик и позволяющий проводить сравнительный анализ PKI-систем и определять рекомендации по повышению их эффективности.

Практическая значимость работы определяется тем, что основные положения, выводы, рекомендации, модели, методы и алгоритмы ориентированы на широкое использование предприятиями и организациями любой структуры, ведомственной принадлежности и формы собственности для оценки потребительского качества экономических информационных систем, использующих инфраструктуру открытых ключей.

Апробация и внедрение результатов исследования. Основные положения и выводы диссертационной работы обсуждались на научных конференциях:

- Региональная конференция «Статистика в современном мире: методы, модели, инструменты» (г. Ростов-на-Дону, 18 мая 2009 г.);

- X международная научно-практическая конференция «Экономико-организационные проблемы проектирования и применения информационных систем» (г. Кисловодск, 17-21 декабря 2008 г.);
- II Межрегиональная научно-практическая конференция «Проблемы создания и использования информационных систем и технологий» (г. Ростов-на-Дону, 18 ноября 2008 г.);
- Десятая международная научно-практическая конференция «Информационная безопасность – 2008» (г. Таганрог, 24-27 июня 2008 г.);
- Третья всероссийская научно-практическая интернет-конференция профессорско-преподавательского состава «Проблемы информационной безопасности» (г. Ростов-на-Дону, 9-16 июня 2008 г.).

Основные положения, полученные в результате проведенного исследования, используются при чтении курсов специальности «Организация и технология защиты информации» («Защита информационных процессов в компьютерных системах», «Безопасность систем электронной коммерции») и специальности «Прикладная информатика» («Информационная безопасность») в Ростовском государственном экономическом университете (РИНХ).

Отдельные результаты диссертационной работы использованы при анализе PKI-системы ООО «НПП «ЭСТОК»». Также некоторые направления представленного научного исследования реализовывались в рамках НИР на тему «Разработка инструментальных методов анализа качества распределенной PKI-инфраструктуры» по договору с РГЭУ «РИНХ» №14/09–ВН от 10.09.2009 г. Документы, подтверждающие внедрение, прилагаются к диссертации.

Публикации. По результатам диссертационного исследования опубликовано 10 печатных работ, 2 из которых – в изданиях, рекомендованных ВАК, общим объемом 2,18 п.л.

Структура работы. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулированы цели и задачи исследования, определены объект, предмет и методы исследования, приведены элементы научной новизны.

В первой главе «Концепция инфраструктуры открытых ключей» рассмотрены принципы симметричной и асимметричной криптографии. Сильной стороной симметричных криптоалгоритмов является их надежность, стойкость и высокая скорость обработки. Слабой стороной – работа с секретными ключами, для передачи которых требуется надежный канал связи.

Скорость работы в асимметричных криптосистемах ниже, чем в симметричных, но они отличаются более удобными правилами обмена ключей, что позволяет сократить число передаваемых ключей почти в 2 раза.

В инфраструктуре открытых ключей были выделены субъекты, объекты, функции и модули. Субъекты PKI включают владельцев сертификатов, пользователей сертификатов и доверенные центры, осуществляющие сертификацию открытых ключей. Объектами PKI являются сами сертификаты, списки отозванных сертификатов. Функции PKI обеспечивают необходимое управление объектами и их использование в прикладных системах. Модули PKI представляют собой структурные составляющие удостоверяющего центра.

Инфраструктура открытых ключей представляет собой совокупность программно-аппаратных средств и организационно-технических мероприятий, в число которых входят государственные и международные стандарты в области криптографии и защиты информации, нормативные документы, составные элементы PKI-систем и приложения.

Основой PKI-системы является удостоверяющий центр (УЦ), который может состоять из обязательного компонента – Центра сертификации, опциональных компонентов – Центра регистрации, Хранилища сертификатов (репозитория) и других модулей.

Структура PKI-системы имеет иерархический вид – от простой до весьма сложной структуры. Однако можно выделить 2 вида иерархии: открытую, в которой корневой сертификат выдан сторонней доверенной организацией, и частную, где корневой сертификат является самоподписанным и используется тольво внутри данной PKI-системы.

При взаимодействии УЦ между собой возникает проблема установления доверия между ними. Существуют 4 модели доверия: иерархическая, сетевая, мостовая и гибридная. Каждая из этих моделей предназначена для организации эффективной структуры PKI-системы. Выбор модели доверия является первым шагом при проектировании УЦ.

Дополнительной службой, строящейся также на основе УЦ, является электронный нотариат, целью которого является установление доверия в тех случаях, когда технически это сделать невозможно, в силу различия в стандартах шифрования, алгоритмах и пр.

Программное обеспечение является важнейшим компонентом PKI-системы. От его функциональных возможностей и качества работы зависит эффективность работы удостоверяющего центра. Поэтому следующим шагом стал анализ следующих программных продуктов: Baltimore UniCert, Entrust Authority™, Microsoft Certificate Services, Red Hat Certificate System (бывший Netscape Certificate System), Novell Certificate Server, RSA Digital Certificate Solutions (бывший RSA Keon), Удостоверяющий Центр «КриптоПро УЦ».

Одним из результатов анализа стал перечень типовых функций, наиболее характерных для PKI-систем. Функции стали исходными данными для дальнейшего анализа.

Во второй главе «Методы оценки характеристик PKI-систем» исходя из функций PKI-систем составлен перечень функциональных и элементарных операций. Последние раскрывают содержание ФО до уровня протоколов.

ФО были распределены по группам, согласно областям, где они находят свое применение: электронный документооборот, электронный нотариат,

служба штампов времени, банкинг (система банк-клиент), электронные торги, электронные платежи. Так как некоторые операции являются неотъемлемыми для каждой из областей, они были выписаны отдельно. Они являются основой для дальнейшего анализа.

Путем эксперимента на стендовой PKI-системе нами были получены начальные данные о времени выполнения элементарных операций. Число элементарных операций в нашем случае более 300, поэтому случайная сумма времени их выполнения, согласно центральной предельной теореме, будет иметь распределение, близкое к нормальному.

Одна из областей применения PKI-систем – электронный документооборот. Перечень функциональных операций в области электронного документооборота приведен в таблице 1.

Таблица 1 – Перечень функциональных операций в области электронного документооборота

1.	Регистрация участника ЭД
2.	Авторизация участника в системе
3.	Заполнение/изменение данных пользователя
4.	Формирование секретной ключевой информации
5.	Формирование запроса на сертификат
6.	Отправка запроса на сертификат
7.	Изготовление сертификата открытого ключа
8.	Вывод копии сертификата на печать
9.	Аннулирование (отзыв) сертификата открытого ключа по запросу пользователя
10.	Приостановление действия сертификата открытого ключа
11.	Возобновление действия сертификата открытого ключа
12.	Перевыпуск сертификата
13.	Запрос сертификата произвольного участника ЭД
14.	Проверка статуса сертификата
15.	Проверка статуса сертификата по дереву отозванных сертификатов
16.	Получение списка отозванных сертификатов
17.	Получение дельта-списка отозванных сертификатов
18.	Доказательство обладания закрытым ключом, соответствующим открытому ключу
19.	Составление и сохранение произвольного документа

20. Прикрепление файла к документу
21. Постановка ЭЦП под документом
22. Проверка ЭЦП под документом
23. Отправка документа на рассмотрение/согласование
24. Отправка документа на подпись электронному нотариусу
25. Получение информации об объекте, заверенном нотариусом
26. Пакетный ввод документов
27. Списание документа в дело и передача в архив
28. Создание пользовательского напоминания
29. Поиск документа по различным реквизитам
30. Поиск дубликата документа
31. Подготовка и печать журналов регистрации документов

Источник: авторский.

Исходя из этого была рассчитана трудоемкость выполнения группы ФО в области электронного документооборота. Однако полученный результат не учитывает частоты обращения к ФО на практике. В связи с этим модель вычисления трудоемкости была усовершенствована.

С помощью формул (1) и (2) были рассчитаны характеристики нормального распределения, и при помощи интегральной фунции Лапласа вычислена вероятная трудоемкость выполнения группы ФО в области электронного документооборота с учетом частот обращения к ФО.

$$M(X_j)=q_1 \cdot M(x_1)+q_2 \cdot M(x_2)+q_3 \cdot M(x_3)+...+q_N \cdot M(x_N) \ , \qquad (1)$$

$$\sigma(X_j)=\sqrt{\sum_{j=1}^{N} q_j \cdot D(x_j)} \ . \qquad (2)$$

где q_i, q_j - частоты использования i-й и j-й функциональных операций,

$M(x_j)$ – математическое ожидание i-й функциональной операции,

$D(x_j)$ – дисперсия j-й функциональной операции.

Так расчет показал, что группа функциональных операций в области электронного документооборота в 94,82% случаев будет выполнена за время между 813 и 834 секундами.

Также был предложен подход к оценке характеристик PKI-систем с учетом последовательностей (транзакций) функциональных операций

последовательности ФО, строго следующих друг за другом и приводящих пользователя к желаемому результату.

Как минимум один раз в 2 года пользователь обязан сменить сертификат открытого ключа подписи с целью безопасности. Таким образом, можно определить следующие транзакции, которые приводят к смене одного сертификата другим.

В первую очередь определяются обязательные транзакции, без которых невозможна работа PKI-системы. Часть из них приведена ниже.

Перевыпуск сертификата
3 → 5 → 6 → 7 → 8 → 9 → 10 → 11 → 43 → 44 → 45 → 46
Перевыпуск сертификатов (в пакетном режиме)
3 → 18 → 19 → 20 → 21 → 22 → 25 → 43 → 44 → 45 → 46
Приостановка действия сертификата
3 → 12 → 43 → 44 → 45 → 46
Приостановка действия сертификатов (в пакетном режиме)
3 → 23 → 43 → 44 → 45 → 46
Возобновление действия сертификата
3 → 13 → 43 → 44 → 45 → 46
Приостановка действия сертификатов (в пакетном режиме)
3 → 24 → 43 → 44 → 45 → 46

Здесь вместо наименований мы используем номера функциональных операций, полный перечень которых приведен в Приложении Г.

Другие транзакции связаны непосредственно с той областью, где они применяются.

Заверение документа у электронного нотариуса
3 → 26 → 27 → 28 → 47 → 49 → 39 → 38 → 29
Заверение документа у электронного нотариуса с выдачей метки времени
3 → 26 → 27 → 28 → 50 → 53 → 51 → 47 → 49 → 39 → 38 → 29

Получение юридически значимой метки времени
3 → 53 → 51 → 50 → 28

Покупка товара через систему электронных торгов
3 → 65 → 66 → 68 → 71 → 70

Работа с документами в системе банк-клиент
4 → 54 → 58 → 56 → 47 → 49 → 50 → 51 → 52 → 53 → 46 → 48

Для каждой из транзакций на основании трудоемкости выполнения каждой ФО возможно построить функцию распределения вероятности, с помощью которой определить пределы колебаний трудоемкости при выполнении транзакции.

Так для транзакции «Заверение документа у электронного нотариуса с выдачей метки времени» функция распределения будет иметь следующий вид:

$$\Phi\left(\frac{x-m}{\sigma}\right)=\Phi\left(\frac{x-163,75}{5,34}\right), \quad (3)$$

где Φ – интегральная функция распределения Лапласа;

m – математическое ожидание совместного распределения ФО;

σ – среднее квадратическое совместного распределения ФО.

Результатом рассчета стал интервал времени от 148 до 179 секунд. Трудоемкость выполнения указанной транзакции «Заверение документа у электронного нотариуса с выдачей метки времени» будет находиться внутри этих пределов с вероятностью 99,7%.

В третьей главе «Совершенствование структуры PKI-систем» был построен программный кластер PKI-систем, приведены варианты организации его структуры и на основании особенностей PKI-системы выбрана конкретная реализация – система высокой готовности с единой реплицируемой базой данных.

PKI-система может состоять из нескольких удостоверяющих центров, каждый из которых является самостоятельной системой с определенной структурой. Так что конечный пользователь при обращении к серверу на самом деле контактирует с целой системой УЦ.

Известны 3 вида организации структуры кластеров: высокоскоростные системы, системы высокой готовности и смешанные.

В высокоскоростных системах основным требованием, предъявляемым к решаемой задаче, является возможность разбиения исходной задачи на подзадачи. Тогда при высоком быстродействии узлов системы и каналов,

связывающих эти узлы, достигается необходимая производительность кластера. Однако функциональные операции, которые рассматривались во второй главе, не предусматривают разделения на подзадачи. Таким образом, использование высокопроизводительных систем не дает ощутимого преимущества в виде увеличения производительности, так как узел, принявший запрос, не может понизить свою нагрузку за счет других.

Напротив, использование систем высокой готовности обосновано, поскольку каждый узел будет обрабатывать запрос самостоятельно от начала и до конца. Такое построение позволяет эффективно использовать аппаратные возможности в совокупности с высокой отказоустойчивостью.

На рисунке 1 изображена схема построенной PKI-системы. Каждый ее узел располагает собственной базой данных хранилища сертификатов, к которой направляются все запросы на выборку, в то время как запросы на обновление данных перенаправляются в Хранилище сертификатов. После обновления в Хранилище сертификатов реплицируемые базы данных в каждом из узлов динамически обновляются.

Рисунок 1 – Архитектура PKI-системы с репликацией хранилища

Источник: авторский

Для исследования характера процессов, происходящих внутри PKI-системы, с целью выработки рекомендаций по рациональному построению программного кластера, мы использовали теорию массового обслуживания.

Применение систем массового обслуживания (СМО) с отказами и с ожиданием позволяет вычислить величину необработанных (отвергнутых) запросов к PKI-системе, а также ответить на вопрос об эффективном количестве узлов системы, распределяющих нагрузку между собой.

Для каждой из моделей СМО при заданных условиях были расчитаны показатели эффективности работы PKI-системы. СМО с ожиданием дает больше возможностей для манипулирования системой и позволяет эффективнее управлять затратами.

Используемая PKI-система состоит из 4-х узлов и в течение минуты ей в среднем приходится принимать 20 заявок. Вероятность отказа в обслуживании в таких условиях составляет более 34%. Для уменьшения числа отказов до 5% необходимо увеличить количество узлов в системе или расширить длину очереди.

Выберем пару параметров — число узлов n и максимальная длина очереди m. Также как и в предыдущем случае необходимо достичь пропускной способности не менее 95%, с тем отличием, что мы можем менять не только число узлов, но и длину очереди. Для этого будем последовательно перебирать значения n и m, пока не достигнем требуемого результата

Результаты расчетов относительной пропускной способности для PKI-системы на заданном числе узлов и длине очереди приведены в таблице 2.

Таблица 2 – Относительная пропускная способность в PKI-системе

Число узлов в PKI-системе	**Максимальная длина очереди**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
4	0,65	0,69	0,71	0,73	0,74	0,75	0,76	0,76	0,76
5	0,76	0,80	0,83	0,85	0,87	0,88	0,89	0,90	0,90

6	0,85	0,89	0,91	0,93	0,94	***0,95***	***0,96***	***0,97***	***0,97***
7	0,91	0,94	***0,96***	***0,97***	***0,98***	***0,98***	***0,99***	***0,99***	***0,99***
8	***0,95***	***0,97***	***0,98***	***0,99***	***0,99***	***0,99***	***1,00***	***1,00***	***1,00***

Источник: авторский.

Из таблицы видно, что для достижения поставленной цели возможно использовать два различных варианта. С одной стороны, можно увеличить длину очереди, что существенно сократит расходы, но понизит качество предоставляемых услуг. С другой стороны, увеличение числа узлов позволит сократить очередь до 1 единицы, что ведет к противоположному результату. Доступны также и другие компромиссные варианты.

Поставленная задача может быть решена как задача линейного целочисленного программирования, с тем отличием, что ограничение имеет нелинейный вид и не может быть представлено в непрерывном виде (из-за присутствия факториала).

Применение целочисленного программирования позволит составить целевую функцию, учитывающую расходы на увеличение числа узлов, а также учесть потери связанные с увеличением размера очереди.

Целевая функция была составлена из расчета, что средняя стоимость современного сервера равна 300 тыс. рублей (2xE7430-12mb / 4x1Gb (16DIMM Slots) / no SFFHDD (8/16) / RAID (P400 256Mb) / 2xGigNIC / DVD). Именно на эту величину увеличатся общие единовременные затраты при увеличении числа узлов на 1 единицу.

Также здесь следует учесть величину штрафа за увеличение размера очереди на одну единицу. Это могут быть затраты, связанные с модернизацией аппаратного и программного обеспечения, оттоком клиентов в связи с увеличением времени ожидания в очереди, а также служащие фиктивным ограничением на длину очереди.

$$\begin{cases} Z(x)=300n+50m\to min, \\ Q\geq 0{,}95, \\ n\geq 4, \\ m\geq 1, \\ n,m\in \mathbf{N} \end{cases} \quad (4)$$

где Z – оптимизируемая функция;

Q – относительная пропускная способность;

n – количество узлов в системе;

m – количество мест в очереди.

Для решения задачи (3) был выбран графический вариант решения с использованием метода последовательного перебора для области допустимых решений. Это наиболее приемлемый способ, поскольку он позволяет избежать сложных расчетов в ограничениях.

Для этого на рисунок наносятся точки из области допустимых значений и линия, соответствующая Z = *const*, и указывается направление ее убывания.

Рисунок 2 – Графическое решение задачи

Источник: авторский.

Из рисунка 2 видно, что оптимизируемая функция достигает минимального значения Z_{min} = 900 в точке (6,6). Следовательно, достаточно увеличить количество узлов на 2, а размер очереди на 5 мест, чтобы решить

поставленную задачу. При этом затраты на ввод в эксплуатацию двух новых узлов составят 600 тыс. рублей.

Для сравнения PKI-систем между собой был построен обобщенный профиль. В него были включены функциональные операции и трудоемкость их выполнения.

Следует отметить, что сравнению подлежат системы, в которых полностью совпадают перечни обязательных ФО. Это выступает критерием сравнимости PKI-систем. Обязательные ФО обеспечиваются средствами УЦ, на основе которого строится любая PKI-система. Такое требование позволяет сравнить практические любые системы по трудоемкости. Профиль PKI-системы схематически изображен на рисунке 3.

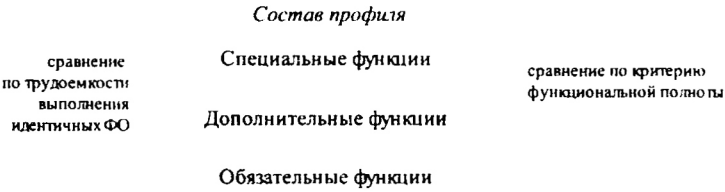

Рисунок 3. Состав и структура профиля PKI-системы

Источник: авторский.

Первоначально профиль формируется из стендовой системы, после чего он накладывается на другие системы. Каждое использование профиля сопровождается его изменением, в результате чего он становится эталонным.

Эталонный профиль PKI-системы может быть использован для формирования общей оценки любой другой системы, а также для получения рекомендаций по улучшению качества предоставляемых услуг, что выражается через ФО, или уменьшению трудоемкости по отдельным ФО.

Сравнение PKI-системы с профилем проходит в 2 этапа:

- сравнение по критерию функциональной полноты;
- сравнение по трудоемкости выполнения ФО.

Для сравнения PKI-систем по критерию функциональной полноты необходимо, чтобы системы принадлежали одной и той же области применения.

В первом случае используется методика проф. Г.Н. Хубаева[1], которая позволяет высказаться о соответствии исследуемой системы профилю объекта и выразить это количественно при помощи меры подобия Жаккарда.

Во втором — нахождение разности во времени выполнения операций между схожими показателями позволяет дать общую оценку скорости работы PKI-системы, а также указать на конкретные ФО, которые в профиле реализуются быстрее.

В диссертационной работе были рассмотрены следующие программные средства: Microsoft CA, OpenCA и Digital Certificate Solutions. Для каждой из PKI-систем были рассчитаны соответствующие величины ($P^{(11)}$, $P^{(10)}$, $P^{(01)}$, $P^{(00)}$) – и вычислена мера подобия Жаккарда.

Результаты сравнительного анализа приведены в таблице 3.

Таблица 3 – Сравнительный анализ PKI-систем с Профилем

PKI-система	$P^{(11)}$	$P^{(10)}$	$P^{(01)}$	$P^{(00)}$	Мера подобия Жаккарда, G
Microsoft CA	3	9	1	13	0,23
OpenCA	10	2	2	14	0,71
Digital Certificate Solutions	11	1	1	13	0,85

Из таблицы видно, что Microsoft CA значительно проигрывает остальным PKI-системам. Причина такого результата кроется в отсутствии функциональных операций связанных с пакетной обработкой сертификатов. Меры Жаккарда OpenCA и Digital Certificate Solutions можно считать достаточно соответствующими профилю, особенно с учетом того, что в PKI-системах присутствуют функциональные операции, не включенные в Профиль.

[1] Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы (Software & Systems). 1998. - № 2. - С. 6–9.

В заключении диссертационной работы приведены основные выводы по результатам проведенного исследования.

По теме диссертации автором опубликованы следующие работы:

Статьи в периодических научных изданиях, рекомендуемых ВАК для публикации научных работ, отражающих основное научное содержание диссертаций:

1. Коротаев Н.В. Анализ программных средств реализации криптопротоколов в современных удостоверяющих центрах // Вестник РГЭУ «РИНХ», – 2008. – № 2 (26). – С. 315–321. – 0,29 п.л.

2. Тищенко Е.Н., Коротаев Н.В. Оптимизация числа узлов распределенной PKI-системы // Экономические науки. – 2009. – № 9 (58). – С. 341–344. – 0,27 п.л., в т.ч. авторских 0,17 п.л.

Статьи в журналах, сборниках научных трудов и сборниках материалов докладов конференций:

3. Коротаев Н.В. Проблема выбора систем электронного документооборота // Проблемы информационной безопасности: Материалы II Всерос. науч.-практ. интернет-конф. профессорско-преподават. состава (14-18 мая 2007 года) / РГЭУ «РИНХ». — Ростов н/Д, 2007. — С. 129–131. 0,13 п.л.

4. Коротаев Н.В. Современные проблемы криптоанализа и стойкости криптоалгоритмов // Вопросы экономики и права: Сб. ст. аспирантов и соискателей уч. степ. канд. наук. / РГЭУ «РИНХ». — Ростов н/Д, 2007. – Вып. 5. — С. 132–135. – 0,21 п.л.

5. Коротаев Н.В. О характеристиках некоторых стандартизированных криптоалгоритмов // Информационные системы, экономика, управление трудом

и производством: Уч. зап. / РГЭУ «РИНХ». — Ростов н/Д, 2007. – Вып. 11. — С. 132–141. - 0,33 п.л.

6. Коротаев Н.В. Факторы обеспечения безопасности электронного правительства // Ваш капитал. Деловой аналитический журнал. — 2008. – № 4–5 (73–74). – С. 34–36. – 0,22 п.л.

7. Коротаев Н.В. Применение теории надежности для оценки защищенности информационных систем // Информационная безопасность: Материалы X Междунар. науч.-практ. конф. / Таганрог: Изд-во ТТИ ЮФУ, 2008. – Ч. 1. — С. 78–79. – 0,12 п.л.

8. Коротаев Н.В. Сравнение эффективности сжатия информации различными программными продуктами // Вопросы экономики и права: Сб. ст. аспирантов и соискателей уч. степ. канд. наук. / РГЭУ «РИНХ». — Ростов н/Д, 2008. – Вып. 6. — С. 101–106. – 0,20 п.л.

9. Коротаев Н.В. Расчет вероятного времени выполнения группы функциональных операций в области электронного документооборота // Статистика в современном мире: методы, модели, инструменты: Материалы регион. науч.-практ. конф. / РГЭУ «РИНХ». — Ростов н/Д, 2009. — С. 147–149. – 0,13 п.л.

10. Коротаев Н.В. Сравнительный анализ программных средств сжимающего кодирования информации // Проблемы информационной безопасности: Материалы IV Всерос. науч.-практ. интернет-конф. (9-15 июня 2009 года) / РГЭУ «РИНХ». — Ростов н/Д, 2009. — С. 134 -144. – 0,38 п.л.

Подписано в печать 18.11.2009.

Печать цифровая. Бумага офсетная. Гарнитура «Times New Roman».

Формат 60x84/16. Объем 1,0 уч.-изд. л. Тираж 120 экз.