На рис. 6 представлена линейная регрессионная зависимость от расстояния относительных погрешностей прогнозирования с помощью нормированных значений сроков доставки груза.

Эта зависимость показывает, что погрешность на большом интервале расстояния доставки груза практически постоянная, но достаточно большая.

## Заключение

Исследования показали, что ошибка в прогнозировании срока доставки груза железнодорожным транспортом по нормированным данным в среднем составляет 40 % (рис. 6) и максимально может доходить до 55 % (табл. 4).

**Библиографический список**

1. **Правила** исчисления сроков доставки грузов железнодорожным транспортом от 18 июня 2003 г. № 27. – Москва, 2003.

2. **Методика** оценки вероятности своевременной доставки груза железнодорожным транспортом / Г. Б. Титов // Изв. ПГУПС. – 2013. – Вып. 2 (35) – С. 81–86.

3. **Оценивание** рисков необеспечения своевременной доставки груза железнодорожным транспортом / П. В. Герасименко, Г. Б. Титов // Материалы 8-й Междунар. науч.-практич. конф. – Киев : Гос. экономико-технологический ун-т транспорта, 2013. – С. 293–295.

4. **О составе** работ и услуг, входящих в тарифы на перевозки грузов от 7 июля 1998 г. № В-6376. – Москва, 2003.

УДК 004.42

**В. Н. Кустов**
ООО «УЦ Газинформсервис»

**С. А. Кирюшкин, Т. Л. Станкевич**
ООО «Газинформсервис»

# О ПОДХОДАХ К АВТОМАТИЗАЦИИ ПРОЦЕССА АУДИТА ОПЕРАТОРОВ СЕРВИСОВ ДОВЕРИЯ

В настоящее время в РФ соответствие сервисов инфраструктуры открытых ключей требованиям руководящих документов оценивают без применения средств автоматизации. При этом человеческий фактор может стать причиной неточностей, больших временны́х затрат. Также в РФ отсутствует единая система комплексного аудита, необходимая для оценки правильности функционирования всех элементов инфраструктуры открытых ключей. В статье рассмотрен подход к автоматизации системы оценки сервисов, перечислены основные элементы, которые должны подвергаться аудиту в рамках создания системы комплексного аудита. Подобные разработки позволят значительно сократить время проведения сертификационных испытаний, повысить точность оценки системы, выявить причины ошибок.

комплексный аудит, система оценки соответствия, удостоверяющий центр, аудит по WebTrust, Data Validation and Cerification Server (DVCS), валидация пути сертификатов.

## Введение

Вопросы оценки соответствия (входного и периодического текущего контроля) состояния организационно-технических систем установленным руководящими документами требованиям и нормам – неотъемлемая часть создания и функционирования гармонизированных, эффективных информационных систем. Единое пространство доверия (ЕПД) в информационной среде как инфраструктура доверия современного электронного государства, несомненно, должно быть именно такой системой. Однако в РФ к настоящему времени не существует системы комплексного аудита элементов ЕПД (т. е. такого аудита, который охватывал бы техническую, организационную, финансово-экономическую и юридическую составляющие системы), данные которого используются для оценки соответствия. Но есть международные примеры таких решений, к которым относится, прежде всего, программа WebTrust для центров сертификации.

ЕПД представляет собой систему технологических и организационных мероприятий, направленных на обеспечение юридически значимого и безопасного электронного взаимодействия органов власти, юридических и физических лиц как одного, так и нескольких государств с использованием технологии электронной подписи. Основой функционирования ЕПД является Public Key Infrastructure (PKI) – инфраструктура открытых ключей. Чтобы быть уверенными в правильности функционирования всех компонент PKI (центра регистрации, репозитория, центра сертификации, электронного архива длительного хранения), необходимо наличие единой системы технологий оценки соответствия сервисов, представляемых PKI, существующим рекомендациям и стандартам.

Таким образом, базовое понятие ЕПД должно быть расширено и подразумевать как возможность проверки электронной подписи (ЭП) документа, так и единую систему технологий оценки. Единая система технологий оценки необходима для получения международного сертификата, подтверждающего, что процессы в организации соответствуют лучшим мировым практикам. Подобное решение приводит WebTrust в Руководящем документе «Webtrust for certification authorities – extended validation audit criteria». Согласно этому документу, каждый удостоверяющий центр (УЦ), желающий заниматься выпуском сертификатов, должен подвергаться расширенному аудиту независимой третьей стороной (аудитором) [1]. Существуют определенные требования, соответствие которым проверяет аудитор.

## 1 Основные элементы комплексного аудита согласно программе WebTrust для центров сертификации

Основные параметры, которые контролирует аудитор при проведении сертификации УЦ:

1) на своем веб-сайте УЦ и корневой УЦ раскрывают практики, политики и процедуры проверки сертификатов; указывают на свое соответствие руководящим документам. УЦ публикует руководящие документы о порядке отзыва сертификатов, предоставляет пользователям услуг подробные инструкции о порядке действий в случае компрометации закрытого ключа или каких-либо видов мошенничества;

2) УЦ должен стать гарантом того, что информация о пользователе корректно собрана и проверена, а целостность ключей и сертификатов обеспечивается на протяжении всего их жизненного цикла. При этом аудиту подвергаются:

- профиль пользователя;
- содержание сертификата;
- заявки на расширенный сертификат;
- требования к проверке информации (например, проверка юридического существования организации, названия, регистрационного номера; принадлежность к родительской, дочерней компании или филиалу; законность существования и подобное);
- статус сертификата;

• уровень квалификации сотрудников и вопросы третьей стороны;

• вопросы данных и записей (например, процессы генерации, копирования, восстановления, архивации и уничтожения ключей; события управления жизненным циклом криптографических устройств и подобное).

Таким образом, аудит по описанию WebTrust представляет собой комплексный процесс, каждая составляющая которого включает организационные мероприятия, напрямую зависящие от квалификации специалистов, а также техническую составляющую, призванную облегчить работу сотрудников.

## 2 Подход к автоматизации процесса оценки соответствия сервисов требованиям Руководящих документов

Процесс оценки соответствия сервисов УЦ требованиям и стандартам с технической точки зрения можно автоматизировать, что приведет к повышению точности оценок и сокращению времени тестирования и анализа результатов. Автоматизировать процесс можно, например, в виде системы аудита, вносящей записи в журнал событий, и программы – анализатора записей. В программу-анализатор импортируются записи журнала событий, выполняется оценка соответствия полученных результатов тестирования системы эталонам, установленным руководящими документами.

Национальный институт стандартов и технологии США (National Institute of Standards and Technology – NIST) разрабатывает серии криптографических тестов и тестов интероперабельности PKI. Созданные наборы тестов позволяют разработчикам и тестовым лабораториям определять соответствие программ/продуктов PKI стандарту X.509 (стандарт, определяющий форматы данных и процедуры распределения открытых ключей с помощью сертификатов с ЭП, которые предоставляются сертификационными органами – УЦ) [2]. NIST открыто публикует информацию, необходимую для выполнения этих тестов (например, описание каждого теста, ожидаемые результаты теста, любые сертификаты/ключи, списки отозванных сертификатов, необходимые для выполнения тестов и т. п.).

Подобные предложения и соответствующие наборы тестов – это задача, которая требует от разработчиков высокой квалификации и профессионального уровня знаний по предмету тестирования. Соответственно, и автоматизация процесса тестирования системы предполагает высокую сложность и трудоемкость, требует соответствующих знаний и привлечения высококвалифицированных специалистов.

До настоящего времени проверку соответствия продуктов требованиям и стандартам выполняют вручную.

В практике российской PKI, пожалуй, что-то подобное проводится при выполнении процедур подтверждения соответствия (сертификации, декларировании) продуктов. Специфика при этом такова, что значительная часть требований на соответствие X.509 в РФ отсутствует. Следовательно, можно утверждать, что автоматизированных методик комплексной оценки соответствия в РФ нет. Мы же в данной работе ориентируемся на широкий спектр PKI-функционала, что, как известно, лежит далеко за рамками отечественного регулирования. Между тем задача создания ЕПД предполагает наличие общих требований по всему спектру функций.

Рассмотрим примеры тестов, которые могут быть автоматизированы.

### 2.1 Автоматизация процесса оценки соответствия сервиса требованиям на примере Data Validation and Certification Server

В инфраструктуре открытых ключей существует такое требование к сервису доверенной третьей стороны Data Validation and Certification Server (DVCS – сервис, обеспечивающий подтверждение действительности сертификата ключа подписи, удостоверение

обладания информацией в конкретный момент времени и подтверждение электронной подписи документа): «DVCS должен включать строго монотонно возрастающий серийный номер в каждой квитанции». В журнале аудита хранятся записи (квитанции) о полученных результатах обработки запросов к сервису DVCS. Каждая квитанция в зависимости от типа запроса к сервису имеет свой идентификатор. Из журнала аудита (табл. 1) по идентификатору программа-анализатор извлекает соответствующую запись, а из записи – все необходимые данные для выполнения теста (в квитанции содержатся переменные с соответствующим значением). Допустим, серийный номер квитанции сохраняется в записи журнала аудита в качестве значения переменной SerialNumber. Программа-анализатор выбирает из всех событий с идентификатором id = 1 значения переменных SerialNumber и проверяет, что номера квитанций имеют строго возрастающий номер. Блок-схема проверки серийных номеров квитанций представлена на рис. 1.

Согласно приведенной блок-схеме разрабатывается исходный код модуля автоматизации процесса тестирования, который компилируется. Результат выполнения такого теста заносится в шаблон протокола в автоматическом режиме в ходе работы программы-анализатора.

Такие правила анализа предполагается создать по каждому требованию стандартов и рекомендаций для конкретного сервиса (в нашем случае сервиса ДТС – DVCS), что позволит автоматизировать анализ аудита при сертификационных и аттестационных испытаниях.

### 2.2 Автоматизация процесса оценки соответствия сервиса требованиям на примере валидации пути сертификатов

Рассмотрим еще один пример автоматизации процесса оценки соответствия сервисов – проверку валидности пути сертификатов.

Предполагается наличие на сервере УЦ журнала аудита, в котором хранятся записи по каждому запросу к ДТС, в том числе проверка валидности цепочки сертификатов. При этом каждая запись хранит значения переменных, использованных в проверке пути. Программа-анализатор извлекает из записи (с соответствующим объектным идентификатором, в примере id = 678) все необходимые переменные и затем проверяет ответ, полученный пользователем от УЦ на запрос проверки валидности сертификата, и фактический результат проверки.

Порядок валидации следующий. Прежде чем сертификат станет доверенным, выполняется проверка того, что он получен из надежного источника. Подтверждение пути включает обработку сертификатов открытых

ТАБЛИЦА 1. Журнал аудита

| № п/п (*i*) | Идентификатор запроса (id) | Содержимое квитанции (переменные) |
|---|---|---|
| 0 | 1 | X=…, Y=…, …, SerialNumber=… |
| 1 | 1 | X=…, Y=…, …, SerialNumber=… |
| 2 | 4 | X=…, Y=…, …, SerialNumber=… |
| … | … | … |
| *k* – 1 | 1 | X=…, Y=…, …, SerialNumber=… |
| k | 1 | X=…, Y=…, …, SerialNumber=… |

где *k* – число записей в журнале аудита; *i* – *i*-я запись в журнале аудита.

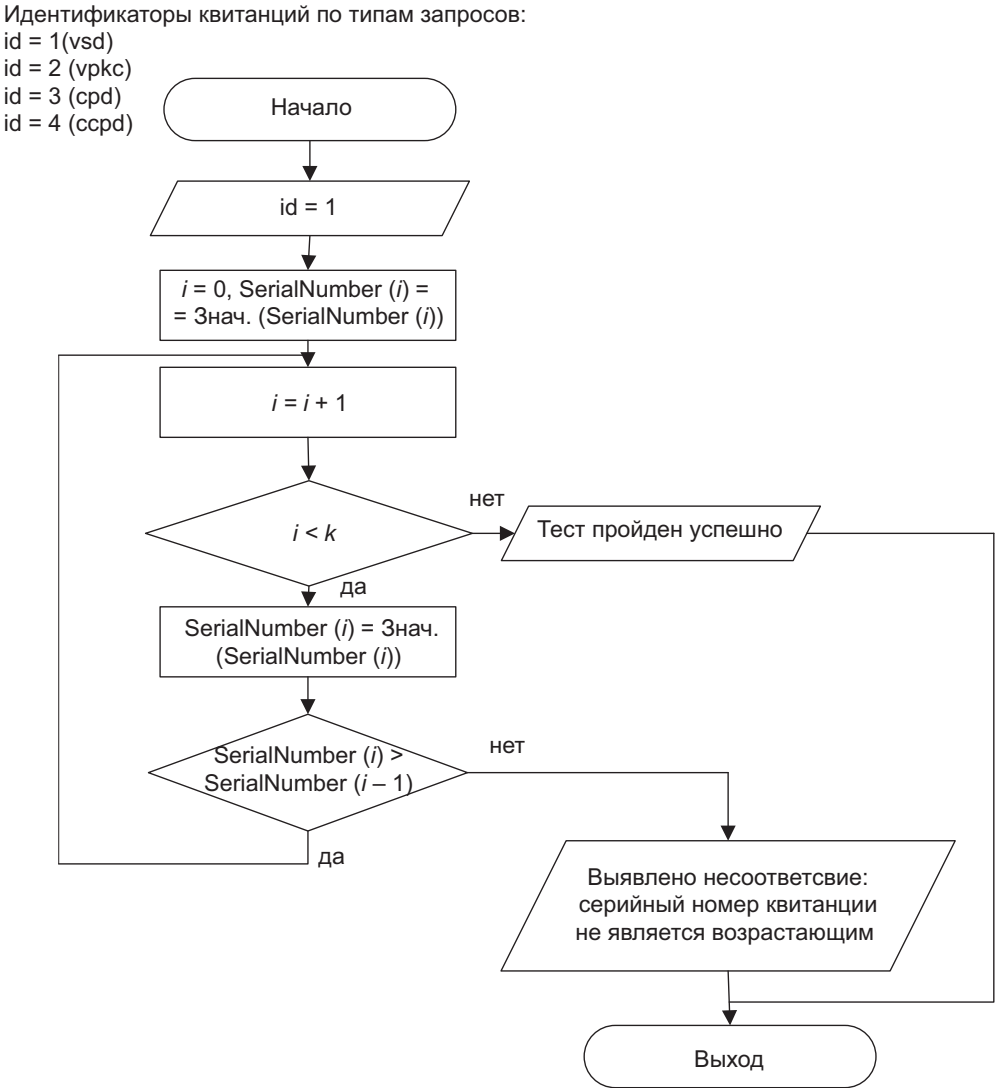


Рис. 1. Блок-схема проверки серийного номера квитанций

ключей и сертификатов соответствующих издателей по иерархической структуре вплоть до завершения пути сертификатов доверенным самозаверенным сертификатом. Если при обработке одного из сертификатов в пути возникает проблема или не удается найти сертификат, путь сертификатов считается ненадежным. Рассмотрим такую проверку более подробно.

Обработка последовательности сертификатов состоит из двух этапов:

1) построение пути, которое заключается в агрегировании всех сертификатов, необходимых для формирования полного пути;

2) валидация пути, которая включает последовательную проверку каждого сертификата последовательности и определение надежности соответствующего открытого ключа.

Путь сертификатов считается валидным, если образующая его последовательность сертификатов удовлетворяет следующим условиям:

1) первый сертификат издан точкой доверия;

2) последний сертификат издан для данного конечного субъекта и содержит данный открытый ключ;

3) имена издателей и субъектов сертификатов образуют последовательность. Во всех сертификатах этой последовательности за исключением первого и последнего имя издате-

ля текущего сертификата совпадает с именем субъекта предыдущего сертификата;

4) период действия всех сертификатов не истек, т. е. все сертификаты последовательности на момент валидации являются действующими.

Этот набор условий необходим, но не достаточен для того, чтобы последовательность сертификатов была валидной. Помимо перечисленных условий должны анализироваться и обрабатываться содержащиеся в сертификатах пути основные ограничения, а также ограничения на имена и политики. Эта обработка выполняется за четыре основных шага:

1) инициализация;

2) базовая проверка сертификата;

3) подготовка следующего сертификата в последовательности;

4) завершение.

На этапе инициализации в зависимости от входных параметров устанавливаются переменные состояния, необходимые для валидации пути сертификатов. В переменных состояния сохраняются различные ограничения, учитываемые при валидации пути. Переменные состояния делятся на четыре группы.

Первая группа переменных состояния используется для сохранения информации, необходимой для верификации ЭП: открытого ключа, связанных с ним параметров и названия алгоритма ЭП (Subject Public Key Information).

Вторая группа переменных состояния предназначена для сохранения информации о цепочке имен и длине пути сертификатов (Path Validation). Переменная состояния отличительного имени ожидаемого издателя (Issuer Alternative Name) используется для подтверждения корректной связи между отличительным именем издателя и отличительным именем субъекта (Subject Alternative Name) в последовательности сертификатов. Переменная состояния длины пути (Path Length) отражает максимальное число сертификатов в последовательности.

Третья группа переменных состояния применяется для сохранения информации о политиках применения сертификатов, образующих последовательность.

Четвертая группа переменных состояния отслеживает правильность именования (Valid Name). Для каждого типа имени должны анализироваться разрешенные и запрещенные поддеревья в иерархической структуре имен.

Как только все переменные состояния инициализированы, осуществляется базовый контроль первого сертификата в последовательности, который включает проверку:

1) срока действия сертификата;

2) статуса сертификата;

3) подписи сертификата;

4) цепочки имен;

5) политики применения сертификатов;

6) ограничений на имена.

ТАБЛИЦА 2. Журнал аудита

| № п/п | Идентификатор запроса (id) | Содержимое квитанции (переменные) |
|---|---|---|
| 0 | 4 | X=…, Y=…, …, SerialNumber=… |
| 1 | 1 | X=…, Y=…, …, SerialNumber=… |
| 2 | 4 | X=…, Y=…, …, SerialNumber=… |
| … | … | … |
| q – 1 | 678 | SubjectPublicKeyInformation=…, ParthValidation=… |
| q | 678 | SubjectPublicKeyInformation=…, ParthValidation=… |

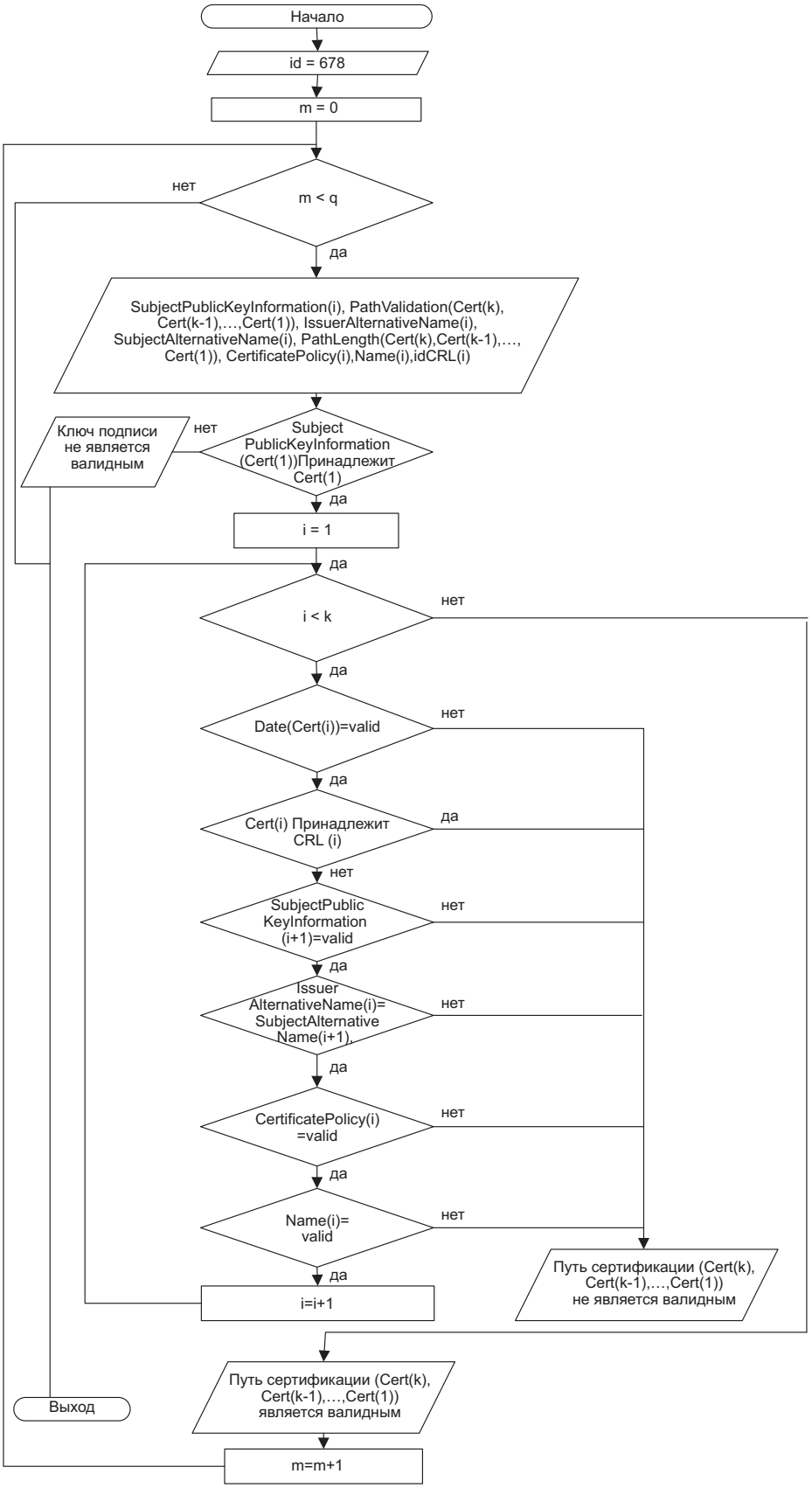


Рис. 2. Блок-схема проверки пути сертификатов

Если хотя бы одна из проверок заканчивается неудачно, то путь сертификатов не признается валидным. Если все проверки завершаются успешно, то происходит переход к следующему сертификату в последовательности и выполняется базовый контроль сертификата.

Блок-схема проверки валидности пути сертификатов (по табл. 2) представлена на рис. 2, где $q$ – число записей в журнале аудита; $k$ – число сертификатов в цепочке; $m$ – $m$-я запись в журнале аудита; $i$ – $i$-й сертификат в цепочке.

**Заключение**

Одной из областей применения подобного средства автоматизации станет труд разработчиков PKI-ориентированного программного обеспечения. Но тогда эти средства автоматизации должны будут сертифицироваться на корректность реализованных проверок и их соответствие семейству стандартов и рекомендаций X.509. Когда у нас будет такой инструментарий, нашим разработчикам это существенно облегчит работу, и мы сможем избежать ситуаций, когда один браузер обрабатывает цепочки сертификатов иначе, чем другой.Таким образом, разработка средств автоматизации оценки соответствия сервисов установленным требованиям и нормам сможет облегчить труд специалистов и сделать результаты тестирований более точными и совершенными, сократить время тестирования системы. Разработка единой системы комплексного аудита элементов ЕПД – это основа создания эффективной, гармонизированной и соответствующей международным стандартам информационной системы.

**Библиографический список**

1. **Webtrust** for certification authorities – extended validation audit criteria. Version 1.4 [Электронный ресурс]. – URL : http://www.webtrust.org/homepage-documents/item72055.pdf (дата обращения 25.03.2014).

2. **Public** key interoperability test suite (PKITS) certification path validation. Version 1.0.1. [Электронный ресурс]. – URL : http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/PKITS.pdf (дата обращения 27.03.2014).

УДК 336.226 (075)

**Е. А. Федоров, Л. Г. Баранова, В. С. Федорова**
Петербургский государственный университет путей сообщения
Императора Александра I

## НАЛОГОВЫЙ КОНТРОЛЬ КАК ЭЛЕМЕНТ НАЛОГОВОГО АДМИНИСТРИРОВАНИЯ

Отношения организации с государством по поводу создания и потребления налоговых платежей выражаются во взаимоотношениях организации с органами государственного управления. В рамках настоящей работы речь идет о взаимоотношениях организации с налоговыми органами в процессе налогового администрирования. Налоговое администрирование рассматривается авторами как комплекс мер по реализации важнейшей задачи налоговых органов – обеспечению поступлений налоговых платежей в бюджет в том объеме, который необходим для финансирования государственных расходов. Для решения этой задачи необходима четко отлаженная и эффективно действующая организация налогового контроля.

налоги, налоговые органы, налоговый контроль, налоговое бремя организации.