Научная статья
УДК 004.056.5
DOI: 10.17853/2587-6910-2024-15-78-90

ИСПОЛЬЗОВАНИЕ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ PKI ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анна Олеговна Чефранова
НОЧУ ДПО ЦПК Учебный центр ИнфоТеКС , Мишина 56 стр 2, г. Москва, РФ, 127083

Аннотация. Статья включает анализ отечественного и зарубежного рынка инфраструктуры открытых ключей и перспективы его роста в ближайшие годы. Рассмотрены причины, обеспечивающие расширение спроса на сервисы PKI. Упомянуты сферы внедрения данных сервисов. Подробно рассмотрены элементы инфраструктуры PKI: электронная подпись, шифрование данных, установление защищенных соединений. Отдельное внимание уделено вопросам выбора архитектуры PKI и соответствующей модели доверия. Сделан вывод о наличии большого числа нерешенных вопросов в этой области. Однако высокий спрос, связанный с развитием банковских сервисов и услуг во всем мире, дает возможность быстро развиваться инфраструктуре открытых ключей во всем мире.

Ключевые слова. инфраструктура открытых ключей, электронная подпись, удостоверяющий центр, безопасность, шифрование

Для цитирования: Чефранова А. О. Использование инфраструктуры открытых ключей PKI для обеспечения информационной безопасности // Новые информационные технологии в образовании и науке. 2024. № 3 (15). С. 78-90 https://doi.org/10.17853/2587-6910-2024-15-78-90

USING THE PUBLIC KEY INFRASTRUCTURE (PKI) TO ENSURE INFORMATION SECURITY

Anna Chefranova
Infotecs Training Center, 56, Mishina st., b.2, Moscow, Russia, 127083

Abstract. The article includes an analysis of the domestic and foreign public key infrastructure market and its growth prospects in the coming years. The reasons for the expansion of demand for PKI services are considered. The areas of implementation of these services are mentioned. The elements of the PKI infrastructure are considered in detail -

electronic signature, data encryption, establishment of secure connections. Special attention is paid to the choice of the PKI architecture and the corresponding trust model. It is concluded that there are a large number of unresolved issues in this area. However, the high demand associated with the development of banking services and services around the world makes it possible for the public key infrastructure to develop rapidly worldwide.

Keywords: public key infrastructure, electronic signature, authentication center, security, encryption, trust model

For citation: Chefranova AO. Using the public key infrastructure (PKI) to ensure information security *New information technoljgies in tducftion and science*. 2024;3(15): 78-90. (In Russ.). doi:10.17853/2587-6910-2024-15-78-90

简评: 文章包括对国内外公开金钥基础建设市场及其未来几年的增长前景的分析。本文讨论了 PKI 服务需求不断增加的原因，并提到了这些服务的实施领域。考虑了 PKI 基础设施的以下元素：电子签名、数据加密、安全连接。特别关注选择 PKI 架构和相应的信任模型的问题。结论是，该领域还存在大量尚未解决的问题。然而，全球范围内银行业务和服务发展的高需求使得公钥基础设施在全球范围内得以快速发展。

主题词： 公开金钥基础建设、电子签名、证明中心、安全、数据加密

Введение

С ростом использования цифровых каналов связи, таких как электронная почта, приложения для обмена сообщениями и онлайн-транзакции, возрастает спрос на инфраструктуру открытых ключей PKI (Public Key Infrastructure), обеспечивающую безопасный способ передачи данных и защиту от киберугроз. Технология PKI обеспечивает безопасную связь с использованием шифрования с открытым и закрытым ключом. Кроме того, PKI помогает проверить личность взаимодействующих сторон.

По мере того как все больше предприятий перемещают свои данные и приложения в облака, потребность в безопасной связи и защите данных возрастает. PKI обеспечивает способ защиты облачных данных и приложений с помощью шифрования и электронной подписи. Это помогает защитить облачные сервисы, предоставляя механизмы аутентификации и авторизации. Оно позволяет пользователям безопасно получать доступ к облачным ресурсам, проверяя свою личность с помощью электронной подписи. Это гарантирует, что только авторизованные пользователи смогут получить доступ к конфиденциальным приложениям и данным. Более того, PKI помогает защитить облачные данные, шифруя их с использованием криптографии с открытым и закрытым ключами. Это гарантирует, что данные не будут перехвачены или прочитаны посторонними лицами. PKI также помогает защититься от атак «человек посередине», обеспечивая безопасность и проверку подлинности связи между облачными службами и пользователями. Таким образом, внедрение облачных сервисов стимулирует спрос на PKI, поскольку предприятиям

необходимо будет подтверждать безопасность своих приложений и данных в облаке [14].

Растущая потребность в гибридной ИТ-инфраструктуре и переход от локальных к облачным решениям PKI приведут к значительному изменению спроса, в том числе на облачные сервисы PKI. Движущей силой для развития таких решений являются строгие правила защиты данных, рост экосистемы устройств Интернета вещей и использование электронных подписей предприятиями.

Сегментация рынка PKI включает в настоящее время аэрокосмическую и оборонную отрасли, здравоохранение, производство, государственные информационные системы, BFSI (Banking, financial services and insurance), образование, розничную торговлю и многие другие сферы. Сегмент BFSI в настоящее время лидирует на рынке за рубежом. Это связано с тем, что данный сектор строго регулируется и требует безопасной связи и защиты данных. PKI широко используется в секторе BFSI для защиты онлайн-транзакций, аутентификации пользователей и защиты конфиденциальных данных. PKI обеспечивает безопасный способ передачи данных через Интернет и защиту от киберугроз, таких как фишинг, взлом и кража личных данных [15].

После вступления в силу Федерального закона РФ № 63 «Об электронной подписи» на российском рынке стала активно создаваться инфраструктура PKI, регулируемая государством [1]. В первую очередь, это делается для внедрения юридически значимого электронного документооборота, который позволит существенно упростить взаимодействие физических и юридических лиц с государственными органами, особенно ведение и сдачу отчетности.

Но использование PKI-решений не ограничивается только государственными органами. Преимущества и возможности инфраструктуры PKI сейчас становятся очевидными и для корпоративного сектора. Инфраструктура открытых ключей необходима коммерческим организациям для безопасного обмена электронными документами и ведения бизнеса, требующего гарантированной защиты электронных транзакций и доступа к данным через Интернет [10].

PKI создает инфраструктуру безопасности, которая позволяет участникам электронного взаимодействия удостовериться:

- в подлинности сторон, участвующих во взаимодействии, их однозначной идентификации;
- в конфиденциальности той информации, которой они обмениваются;
- в целостности информации и неотрекаемости от нее ее владельцами;
- в недоступности информации другим лицам.

Традиционными сферами применения инфраструктуры PKI в настоящий момент являются банковские системы (в частности, e-banking), электронная торговля, биллинговые системы, системы мобильных платежей, системы обработки веб транзакций.

Для понимания проблематики внедрения и развития PKI целесообразно рассмотреть элементы и сервисы данной инфраструктуры, обратив внимание на вопросы практического характера, таки как выбор той или иной архитектуры PKI и соответствующей модели доверия.

1. Инфраструктура PKI

Инфраструктура открытых ключей PKI представляет собой комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам через создание сертификатов и поддержание их жизненного цикла.

В основе инфраструктуры открытых ключей лежит асимметричная криптография, при использовании которой у каждого пользователя имеется пара ключей (закрытый и открытый ключи) и сертификат. Пользователи инфраструктуры PKI хранят свой закрытый ключ в секрете, а открытый ключ свободно распространяют вместе с сертификатом, чтобы другие пользователи имели к нему доступ. Сертификат, в свою очередь, является электронным документом, который подтверждает принадлежность открытого ключа владельцу сертификата, и выдается удостоверяющим центром.

Внедрение PKI позволяет решать широкий круг задач, основными из которых являются:

- электронная подпись;
- шифрование данных;
- установление защищенных соединений по протоколу TLS/SSL [13].

Основными направлениями использования PKI являются: аутентификация, услуги регистрации, инвентаризация цифровых удостоверений, безопасный роуминг, самостоятельное восстановление данных и самостоятельная регистрация в системах с использованием PKI.

2. Электронная подпись

Электронная подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе. Она является результатом криптографического преобразования информации с использованием закрытого ключа и позволяет обеспечить [5]:

- подлинность — однозначно идентифицировать личность лица, подписавшего документ;
- целостность — установить отсутствие намеренного или случайного искажения информации в документе после его подписания;
- неотрекаемость — устранить возможность отказа владельца документа от своей подписи.

Электронная подпись сегодня является наиболее универсальным решением для однозначной идентификации документа, его автора и сторон, его подписавших. Поэтому на основе электронной подписи можно организовать защищенный электронный документооборот и гарантировать достоверность информационного обмена любыми данными [2].

Чтобы получить электронную подпись, необходимо обратиться в удостоверяющие центры [11]. В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» Удостоверяющий центр (УЦ) выполняет следующие функции [1]:

- издает сертификаты ключей проверки электронных подписей (далее — сертификат) и выдает такие сертификаты лицам, обратившимся за их получением;
- устанавливает сроки действия сертификатов;
- аннулирует изданные этим УЦ сертификаты;
- выдает по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП заявителем;
- ведет реестр изданных и аннулированных этим УЦ сертификатов, в том числе включающий в себя информацию, содержащуюся в выданных этим УЦ сертификатах, а также сведения о датах прекращения действия или аннулирования сертификатов и основаниях;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;
- создает по обращениям заявителей ключи ЭП и ключи проверки ЭП;
- проверяет уникальность ключей проверки ЭП в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку ЭП.

Если удостоверяющий центр функционирует в распределенной корпоративной сети и обслуживает большое количество пользователей, то в его состав можно включить центр регистрации. Использование центра регистрации позволяет распределить нагрузку по выдаче сертификатов в удостоверяющем центре, а также производить обслуживание удаленных пользователей [11].

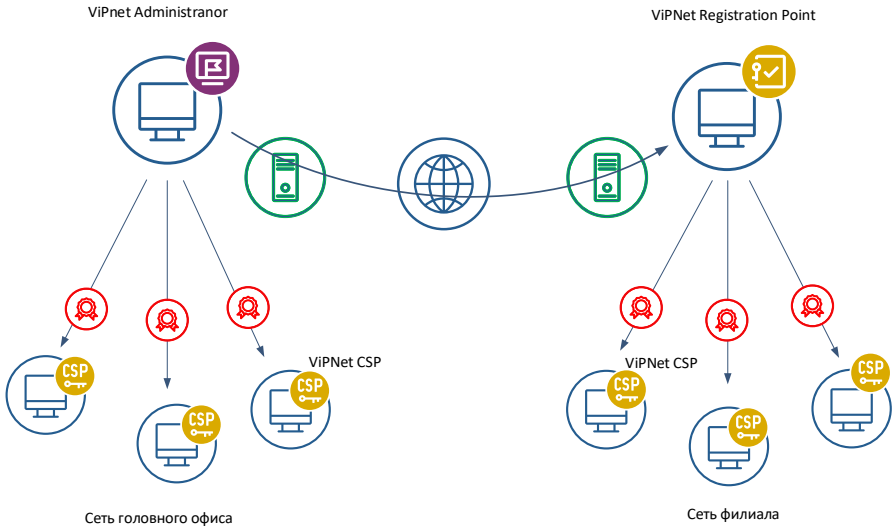

Рис. 1. Сценарий использования центра регистрации

Центр регистрации (RA – Registration Authority) – компонент УЦ, предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты электронной подписи.

Основная задача RA — регистрация пользователей и обеспечение их взаимодействия с УЦ. В задачи Центра Регистрации может также входить публикация сертификатов и списков отозванных сертификатов. ЦР является единственной точкой входа и регистрации пользователей, поэтому только зарегистрированный пользователь может получить сертификат на свой открытый ключ в УЦ.

3. Шифрование данных

Шифрование позволяет обеспечить конфиденциальность данных, то есть их защиту от сторонних лиц. Зашифрованные данные могут надежно храниться или передаваться по открытым каналам связи (например, через Интернет).

В процессе шифрования производится криптографическое преобразование данных с помощью открытого ключа получателя, который доступен публично. Доступ к зашифрованным данным имеет только получатель, потому что только он может расшифровать эти данные с помощью своего закрытого ключа. Для всех остальных лиц зашифрованные данные без закрытого ключа получателя представляют бессмысленный набор символов. Поскольку закрытый ключ не распространяется в процессе взаимодействия и хранится только у получателя, исключается возможность того, что злоумышленник завладеет ключом и расшифрует конфиденциальные данные [4]. С помощью шифрования данных можно обеспечить конфиденциальность любого информационного обмена и тем самым минимизировать риск утечки данных.

4. Установка защищенных соединений по протоколу TLS/SSL

В рамках распространения PKI-технологии появилась возможность устанавливать защищенное взаимодействие между пользователями по различным сетевых протоколам, в частности, по протоколу TLS/SSL. Протокол TLS/SSL дает возможность организовать защищенную передачу данных между узлами корпоративной сети. Он помогает клиент серверным приложениям осуществлять связь в сети таким образом, чтобы предотвратить прослушивание и несанкционированный доступ, а также обеспечить конфиденциальную передачу данных. Это достигается за счет односторонней или двусторонней аутентификации взаимодействующих сторон [13].

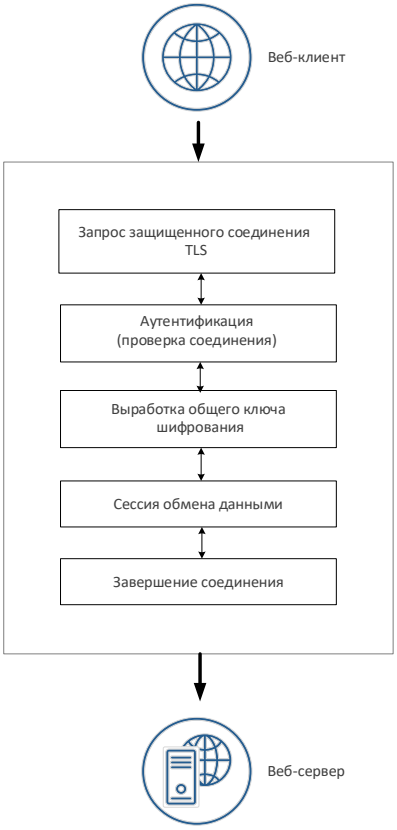

Рис. 2. Установление защищенных соединений

Чаще всего протокол TLS/SSL используется в веб-приложениях, работающих с ресурсами в Интернет, например, в веб браузерах, средствах обмена мгновенными сообщениями, IP телефонии и др.

5. Архитектура PKI

Важным вопросом практического характера является выбор той или иной архитектуры PKI и соответствующей модели доверия.

Архитектура PKI определяет структуру доверия между различными удостоверяющими центрами. Путь доверия – цепочка документов, позволяющая удосто-

вериться, что каждый отдельный сертификат был выдан доверенным удостоверяющим центром. Последним звеном в цепочке является предъявленный сертификат, а самым начальным — сертификат корневого доверенного удостоверяющего центра. При потере доверия к начальному звену в цепочке теряется доверие ко всей цепочке [9].

Для организации взаимодействия различных информационных систем и распространения в них доверия часто требуется организовать совместную работу различных PKI. Например, при межкорпоративном или межведомственном информационном обмене. Обычно используется комбинация нескольких архитектур взаимодействия PKI или одна из этих архитектур:

- простая модель доверия — все пользователи доверяют только одному УЦ, который имеет единый домен доверия;
- иерархическая модель доверия — подчинение нескольких УЦ вышестоящему головному УЦ;
- сетевая модель доверия — объединение одноранговых инфраструктур с кросс-сертификацией головных УЦ;
- мостовая модель доверия — кросс-сертификация каждого УЦ с одним выделенным УЦ-мостом;
- браузерная модель доверия.

5.1. Простая модель доверия

Данной модели доверия соответствует простая архитектура PKI. То есть в такой архитектуре образуются отношения только через единый УЦ и простые пути проверки сертификатов электронной подписи. Данная модель используется в рамках одной организации, где высок уровень доверия к внутренним пользователям. В случае компрометации УЦ, построенного по простой модели доверия, необходим перевыпуск всех сертификатов пользователей [3].

5.2. Иерархическая модель доверия

Данная модель характеризуется прямой иерархией доверительных отношений. Подчиненный УЦ отправляет запрос на издание сертификата в вышестоящий УЦ. Вышестоящий УЦ издает кросс-сертификат и передает его обратно в подчиненный УЦ. В результате УЦ имеет сертификат, изданный по его запросу в вышестоящем УЦ. Головной УЦ имеет только самоподписанный корневой сертификат.

Подчиненные УЦ могут выпускать сертификаты для УЦ, находящихся ниже них по уровню иерархии или для конечных пользователей. В иерархической модели каждая сторона знает и доверяет только открытому ключу подписи головного УЦ. Каждый сертификат может быть проверен путем выстраивания цепочки сертификатов от корневого самоподписанного сертификата головного УЦ.

Иерархическая модель особенно эффективна для организаций с иерархической структурой управления, например, при создании PKI корпоративной или ведомственной информационной системы, когда все владельцы сертификатов в силу трудовых отношений доверяют одному и тому же головному УЦ, и цепочка доверия строится на базе корневого сертификата этого УЦ.

5.3. Сетевая (распределенная) модель доверия

При выстраивании доверительных отношений независимые УЦ издают сертификаты по запросам друг друга и обмениваются ими. В этом случае каждый УЦ распространяет своим пользователям свой собственный корневой самоподписанный сертификат и изданные им кросс-сертификаты других УЦ, с которыми были установлены доверительные отношения.

Пользователь УЦ при проверке сертификата выстраивает цепочку доверия от сертификата УЦ, которому он доверяет и который издал для него сертификат. Преимущество сетевой модели заключается в том, что компрометация одного центра в сети удостоверяющих центров не ведет к утрате доверия ко всей PKI.

5.4. «Мостовая» модель доверия

«Мостовая» модель является частным случаем сетевой модели. При выстраивании доверительных отношений на основе «мостовой» модели выделенный УЦ выступает в роли посредника («моста») между остальными УЦ, связывая их между собой. Для этого «мостовой» УЦ обменивается кросс-сертификатами со всеми остальными УЦ. Однако, в отличие от сетевой модели, «мостовой» УЦ обычно не выпускает сертификаты для конечных пользователей. Также ему не обязательно выпускать корневой сертификат.

«Мостовой» УЦ может устанавливать отношения доверия типа «равный с равным» не только с отдельными УЦ, но и с системами УЦ (пространствами доверия). Если пространство доверия реализовано по иерархической модели, то мостовой УЦ устанавливает связь с корневым УЦ. Если же пространством доверия является сеть УЦ, то мостовой УЦ может взаимодействовать с любым УЦ сети.

Например, УЦ на базе программы ViPNet Удостоверяющий и ключевой центр поддерживает все перечисленные архитектуры и может выполнять для сторонних УЦ следующие роли [12]:

- головного УЦ — обработка запросов от сторонних УЦ и выпуск для них кросс-сертификатов;
- подчиненного УЦ — создание запросов в вышестоящий УЦ и получение от него кросс-сертификата;
- мостового УЦ — выпуск кросс-сертификатов по запросам из сторонних УЦ и создание запросов на кросс-сертификаты в такие УЦ.

5.5. Браузерная модель доверия

Данная модель базируется на популярных браузерах, используемых как средства навигации в Интернете. Эта модель предусматривает встраивание в готовый браузер набора открытых ключей головных удостоверяющих центров, которым пользователь браузера может изначально» доверять «при проверке сертификатов. Браузер позволяет корректировать набор корневых ключей, то есть удалять одни ключи и добавлять другие.

Браузерная модель немедленно делает пользователя браузера доверяющей стороной всех PKI-доменов, представленных в браузере. Для всех практических нужд каждый производитель браузера имеет свой собственный головной УЦ, сертифицирующий «головные» удостоверяющие центры, открытые ключи которых

физически встроены в программное обеспечение браузера. По существу это строгая иерархия с подразумеваемым корнем, то есть производитель браузера является виртуальным головным УЦ, а уровень, находящийся ниже, образуют встроенные в браузер открытые ключи удостоверяющих центров.

Браузерная модель обладает такими преимуществами, как удобство использования и простота обеспечения функциональной совместимости. Данная модель имеет возможность устанавливать отношения доверия между УЦ разного уровня, а также организовывать гибкие связи, которые в случае изменений не приносят значимого ущерба для инфраструктуры PKI.

К недостаткам данной модели можно отнести следующее:

- пользователи браузера автоматически доверяют всем удостоверяющим центрам, открытые ключи которых были заранее встроены в браузер, поэтому безопасность может быть полностью скомпрометирована, если хотя бы один из этих центров окажется «плохим». Причина нарушения безопасности заключается в том, что у пользователя обычно нет уверенности, какой именно корневой ключ из большого числа ключей, встроенных в браузер, участвует
- в проверке сертификата;
- отсутствие практического механизма аннулирования любого из корневых ключей, встроенных в браузер;
- не предусмотрено заключение никакого юридического соглашения или договора между пользователями (доверяющими сторонами) и удостоверяющими центрами, открытые ключи которых встроены в браузер. Так как программное обеспечение браузера часто распространяется свободно или встраивается в операционную систему, удостоверяющие центры не знают, более того, не имеют способа определить, кто является доверяющей стороной.

Определение архитектуры PKI и выбор модели доверия — важные задачи, стоящие перед организацией, использующей или планирующей использовать PKI решения. В настоящее время в РФ есть различные сценарии интеграции подобных разработок в государственные и коммерческие структуры. В ближайшие годы в связи с развитием нормативно-правовой базы в области облачной электронной подписи, потребуется разработка новых средств для обеспечения информационной безопасности облачных сервисов.

Отдельная тема, вызывающая интерес для обсуждения, – это растущее использование HSM (Hardware Security Module), главной целью которого является усиление безопасности PKI [15]. Аналитики рассматривают данные устройства как перспективные и востребованные в ближайшие десять лет. Связано это прежде всего с тем, что HSM — это физические устройства, которые могут быть подключены к сети или интегрированы в сервер и представляют собой безопасное хранилище для криптографических ключей, что предотвращает их экспорт или копирование. Устройства HSM способны выполнять криптографические операции внутри самого модуля, что уменьшает риски, связанные с утечкой ключей при их использовании вне защищенной среды.

В РФ такие устройства уже есть и используются в некоторых организациях. Поэтому закономерно ожидать рост интереса к HSM как у производителей, так и у исследователей.

Заключение

Анализ зарубежных и отечественных источников показал, что технология PKI сих пор очень востребована как за рубежом, так и в нашей стране. Существуют условия для внедрения новых решений в государственном и коммерческом секторах, с целью повышения доверия между различными структурами и уровнями. Производители средств PKI активно развивают линейки продуктов, включая в них последние достижения науки и техники. Интернет вещей и облачные сервисы начинают активно использовать технологии аутентификации, включая электронную подпись, а также все виды работы с ней: издание сертификатов ключей проверки ЭП, поддержание инфраструктуры ключей проверки ЭП. Конечно, еще много нерешенных вопросов в этой области, но высокий спрос, связанный с развитием банковских сервисов и услуг во всем мире, дает возможность быстро развиваться инфраструктуре открытых ключей во всем мире.

Для построения той или иной архитектуры PKI должны быть выработаны организационно-технологические и технические решения, обеспечивающие формирование правовой, организационной, технологической и технической основы реализации механизмов электронной подписи, обеспечивающих юридическую значимость электронных документов при информационном взаимодействии между автоматизированными информационными системами, повышение эффективности бизнес-процессов предприятия, связанных с информационным обменом за счёт использования механизмов ЭП, повышения безопасности информационных ресурсов и процессов их обработки путём использования криптографических средств и сервисов PKI.

Список источников

1. Об электронной подписи: Федеральный закон от 06. 04.2011 г. № 63-ФЗ // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_112701 (дата обращения: 10.01.2025).

2. Вышенский С. В., Григорьев П. В., Дубенская Ю. Ю. Инфраструктура открытых ключей с комплементарной криптографией. IT-ПАРК // Вестник связи. 2007. № 9. С. 138–147.

3. Королёв В. И. Архитектурное построение инфраструктуры открытых ключей интегрированного информационного пространства // Безопасность информационных технологий. 2015. Т. 22, № 3. С. 59–71.

4. Мельников Д. А., Релеев Ю. Ф., Кварацхелия Л. Д. Модель доверия для цифровой экономики Российской Федерации // Безопасность информационных технологий. 2020. Т. 27, № 2. С. 47–64. http://dx.doi.org/10.26583/bit.2020.2.04.

5. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. СПб.: BHV, 2014. 288 с.

6. Петренко С. А. Практика построения PUBLIC KEY INFRASTRUCTURE, PKI // Защита информации. Конфидент. 2002. № 6 (48).

7. Полянская О. Ю., Горбатов В. С. Инфраструктуры открытых ключей. М.: ИНТУИТ, 2013. 367 с.

8. Сабанов А. Г. Аутентификация как составляющая единого пространства доверия // Электросвязь. 2012. № 8. С. 40–44.

9. Сабанов А. Г. Об уровнях доверия к первичной идентификации // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 67–69.

10. Сабанов А. Г., Шелупанов А. А. Идентификация и аутентификация в цифровом мире. М.: Горячая линия – Телеком, 2022. 356 с.

11. Чаплыгин В. Е., Чефранова А. О., Алабина Ю. Ф. Администрирование системы защиты информации ViPNet версии 4. М.: Горячая линия – Телеком, 2020. 188 с.

12. Чефранова А. О., Климонтова Г. Н., Чаплыгин В. Е. Удостоверяющий центр ViPNet. М.: Т8, 2022. 246 с.

13. Чефранова А. О. Технология построения VPN ViPNet. М.: Т8, 2024. 292 с.

14. Public Key Infrastructure (PKI) Market Research Report Information By Solution. URL: https://www.marketresearchfuture.com/reports/public-key-infrastructure-market-3627 (дата обращения: 05.09.2024).

15. Global Public Key Infrastructure (PKI) Market 2023–2027. URL: https://www.researchandmarkets.com/reports/5514882/global-public-key-infrastructure-pki-market (дата обращения: 05.09.2024).

16. Secure Electronic Transaction Specification. The Business De scription. URL: https://www.mbaknol.com/business-finance/secure-electronic-transaction-set/ (дата обращения: 05.09.2024).

17. Secure Electronic Transaction (SET): Definition and How It Works. URL: https://www.investopedia.com/terms/s/secure-electronic-transaction-set.asp (дата обращения: 05.09.2024).

18. Decoding Secure Electronic Transactions (SET). URL: juspay.in/blog/payments/decoding-secure-electronic-transactions (дата обращения: 05.09.2024).

References

1. On Electronic Signature: Federal Law No. 63-FZ dated 04.06.2011. *ConsultantPlyus.* (In Russ.). Accessed January 10, 2025. https://www.consultant.ru/document/cons_doc_LAW_112701

2. Vyshensky SV, Grigoriev PV, Dubenskaya YuYu. Public key infrastructure with complementary cryptography. IT-PARK. *Bulletin of Communications*. 2007;9:138-147.

3. Korolev VI. Architectural construction of the infrastructure of public keys of the integrated information space. *Security of information technologies*. 2015;22(3):59-71.

4. Melnikov DA, Releev YuF, Kvarazcheliya LD. Model of trust for the digital economy of the Russian Federation. *Security of information technologies*. 2020;27(2):47-64. (In Russ.). doi:10.26583/bit.2020.2.04

5. Moldovyan NA, Moldovyan AA. Introduction to public key cryptosystems. St. Petersburg: BHV;2014. 288 c. (In Russ.)

6. Petrenko SA. The practice of building PUBLIC KEY INFRASTRUCTURE, PKI. *Information protection. Confidential.* 2002;6(48). (In Russ.)

7. Polyanskaya OYu, Gorbatov VS. Infra-structures of public keys. Moscow: INTUIT, 2013. 368 p. (In Russ.)

8. Sabanov AG. Authentication as a component of a single trust space. *Telecommunication.* 2012;8:40-44. (In Russ.)

9. Sabanov AG. On the levels of trust in primary identification. *Methods and technical means of information security.* 2018;27:67-69. (In Russ.)

10. Sabanov AG., Shelupanov AA. Identification and authentication in the digital world. Moscow: Hotline - Telecom, 2022. 356 p. (In Russ.)

11. Chaplygin VE, Chefranova AO, Alabina YuF. Administration of the ViPNet information protection system. Moscow: Hotline -Telecom, 2020. 188 p. (In Russ.)

12. Chefranova AO, Klimontova GN, Chaplygin VE. ViPNet Certification Center. Moscow: T8, 2022. 246 p. (In Russ.)

13. Chefranova AO. ViPNet VPN construction technology. Moscow: T8, 2024. 292 p. (In Russ.)

14. Public Key Infrastructure (PKI) Market Research Report Information By Solution. Accessed September 5, 2024. https://www.marketresearchfuture.com/reports/public-key-infrastructure-market-3627

15. Global Public Key Infrastructure (PKI) Market 2023-2027. Accessed September 5, 2024. https://www.researchandmarkets.com/reports/5514882/global-public-key-infrastructure-pki-market

16. Secure Electronic Transaction Specification. The Business De scription. Accessed September 5, 2024. https://www.mbaknol.com/business-finance/secure-electronic-transaction-set/

17. Secure Electronic Transaction (SET): Definition and How It Works. Accessed September 5, 2024. https://www.investopedia.com/terms/s/secure-electronic-transaction-set.asp

18. Decoding Secure Electronic Transactions (SET). Accessed September 5, 2024. juspay.in/blog/payments/decoding-secure-electronic-transactions