Инфраструктура открытых ключей PKI и модели доверия

А.О.Чефранова, д.пед.н., директор Учебного центра
ИнфоТеКС / chefr@infotecs.ru

УДК 004.056.5, DOI: 10.22184/2070-8963.2024.122.6.40.47

Представлен анализ зарубежного рынка инфраструктуры открытых ключей и перспективы его роста в ближайшие годы. Подробно рассмотрены элементы инфраструктуры PKI и модели доверия между удостоверяющими центрами.

Введение

Инфраструктура открытых ключей (PKI – Public Key Infrastructure) обеспечивает безопасный способ передачи данных и защиту от киберугроз. С ростом использования цифровых каналов связи, таких как электронная почта, приложения для обмена сообщениями и онлайн-транзакции, спрос на PKI сильно увеличивается с каждым годом. Данная технология обеспечивает безопасную связь с использованием шифрования с открытым и закрытым ключом. Кроме того, PKI помогает проверить личности взаимодействующих сторон.

По мере того, как все больше предприятий перемещают свои данные и приложения в облачные сервисы, потребность в безопасной связи и защите данных возрастает. PKI обеспечивает способ защиты облачных данных и приложений с помощью шифрования и электронной подписи. Это помогает защищать данные, предоставляя механизмы аутентификации и авторизации, позволяет пользователям безопасно получать доступ к облачным ресурсам, проверяя свою личность с помощью электронной подписи. Использование PKI 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, а также помогает защититься от атак "человек посередине", обеспечивая безопасность и проверку подлинности связи между облачными службами и пользователями. То есть развитие и внедрение облачных сервисов стимулирует спрос на PKI, поскольку организациям необходимо будет подтверждать безопасность своих приложений и данных в облаке. Для примера, аналитики прогнозируют рост зарубежного рынка PKI, который значительно вырастет и к 2032 году составит 21,14 млрд долл. США, а совокупный годовой темп роста составит 18,79% (в течение прогнозируемого периода с 2024 по 2032 годы) [14].

Нужно отметить, что на зарубежном рынке доминирующую роль выполняют сервисы услуг по регистрации открытых ключей. Услуги регистрации необходимы для любого внедрения PKI, поскольку они обеспечивают основу для безопасной связи и защиты любых данных. Без служб регистрации проверка пользователей и устройств и обеспечение того, чтобы только авторизованные стороны имели доступ к конфиденциальным ресурсам, будет очень затруднительно. Со временем, зарубежные аналитики ожидают, что другие сегменты рынка PKI будут расти, так как многие организации, работающие в этой сфере, делают выбор в пользу асимметричных ключевых систем [14].

Иностранные аналитики выявляют растущий спрос на использование устройств HSM (Hardware Security

Module) с целью усиления безопасности PKI. Этот рост рассматривается как одна из основных причин востребованности PKI в течение следующих десяти 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 [15].

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.

В настоящее время зарубежный рынок PKI включает аэрокосмическую и оборонную отрасли, здравоохранение, государственные информационные системы, BFSI (Banking, Financial Services and Insurance), образование, розничную торговлю и многие другие сферы. Лидирующее место на мировом рынке занимает сегмент BFSI. Это связано с тем, что данный сектор строго регулируется и требует безопасной связи и защиты данных. PKI широко используется в данном секторе 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].

Ведущим в ближайшие 10 лет станет североамериканский рынок PKI благодаря широкому внедрению цифровых технологий и сильной нормативно-правовой базе, что уже сейчас привело к высокому спросу на PKI-решения. Сектор банковского дела, финансовых услуг и страхования в Северной Америке является основным конечным пользователем таких решений из-за большого объема финансовых транзакций. Сектор здравоохранения становится активным пользователем решений PKI, так как растет внедрение электронных медицинских записей и приложений для телемедицины.

Ожидается, что будет развиваться быстрыми темпами Азиатско-Тихоокеанский регион, вплоть до 2032 года. Рост здесь стимулируется повышением уровня цифровизации, высоким числом киберугроз и острой потребностью в защите данных из-за большой численности населения и нового уровня внедрения цифровых технологий. Причем наибольшую долю рынка занимает китайский рынок PKI, а самым быстрорастущим в Азиатско-Тихоокеанском регионе является индийский рынок.

В РФ после вступления в силу Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи" на рынке стала активно создаваться инфраструктура PKI, регулируемая государством [1]. В первую очередь, это делалось для внедрения юридически значимого электронного документооборота, который позволил существенно упростить взаимодействие физических и юридических лиц с госорганами, особенно в ведении и сдаче отчетности. Но использование PKI-решений в РФ не ограничивалось только государственными органами. Преимущества и возможности инфраструктуры PKI сегодня стали 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].

Технология 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 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 вебтранзакций и др.

Далее рассмотрим инфраструктуру PKI и то, как она помогает реализовать различные модели доверия.

Инфраструктура открытых ключей

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) 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, главные из которых: 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.

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 подлинность (однозначно идентифицировать личность лица, подписавшего документ), целостность (установить отсутствие намеренного или случайного искажения информации в документе после его подписания) и неотрекаемость (устранить возможность отказа владельца документа от своей подписи) [5].

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 также гарантировать достоверность информационного обмена любыми данными [2].

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 этот ключ не распространяется в процессе взаимодействия и хранится только у получателя, исключается возможность того, что злоумышленник завладеет ключом и расшифрует конфиденциальные данные [4].

Таким образом, с помощью шифрования данных можно обеспечить конфиденциальность любого информационного обмена, и, тем самым, минимизировать риск утечки данных.

Установка защищенных соединений по протоколу TLS/SSL

В рамках распространения PKI-технологии появилась возможность устанавливать защищенное взаимодействие между пользователями по различным сетевым протоколам, в частности, по протоколу TLS/SSL. 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 (рис.1). Это достигается за счет односторонней или двусторонней аутентификации взаимодействующих сторон [13].

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

Удостоверяющий центр

В основе технологии PKI лежит использование сертификатов, которые выдаются и обслуживаются удостоверяющими центрами. Все издаваемые сертификаты заверяются подписью удостоверяющего центра (сертификатом издателя), которая гарантирует их подлинность. Поэтому основным компонентом инфраструктуры PKI является удостоверяющий центр (УЦ) [1, 11].

В соответствии с Федеральным законом № 63-ФЗ УЦ выполняет следующие функции [1]:

- издает сертификаты ключей проверки электронных подписей (далее – сертификат) и выдает такие сертификаты лицам, обратившимся за их получением;

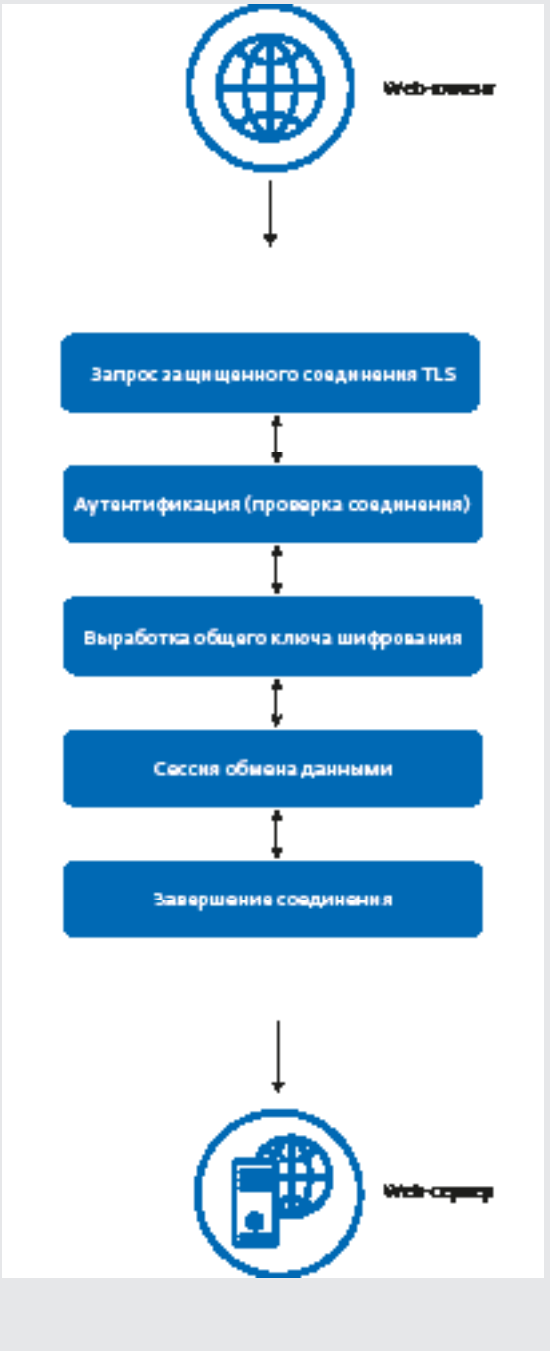

Рис.1. Установление защищенных соединений

- 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 УЦ 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]. На рис.2 представлен сценарий взаимодействия между сетью головного офиса и сетью филиала организации, построенного на основе программного обеспечения ViPNet.

Центр регистрации (ЦР, RA – Registration Authority) – компонент УЦ, предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты электронной подписи. Основная задача ЦР – регистрация пользователей и обеспечение их взаимодействия с УЦ. В задачи ЦР 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.

Архитектура PKI

Архитектура PKI определяет структуру доверия между различными удостоверяющими центрами. Путь доверия – цепочка документов, позволяющая удостовериться, что каждый отдельный сертификат был выдан доверенным УЦ. Последним звеном в цепочке является предъявленный сертификат, а самым начальным – сертификат корневого

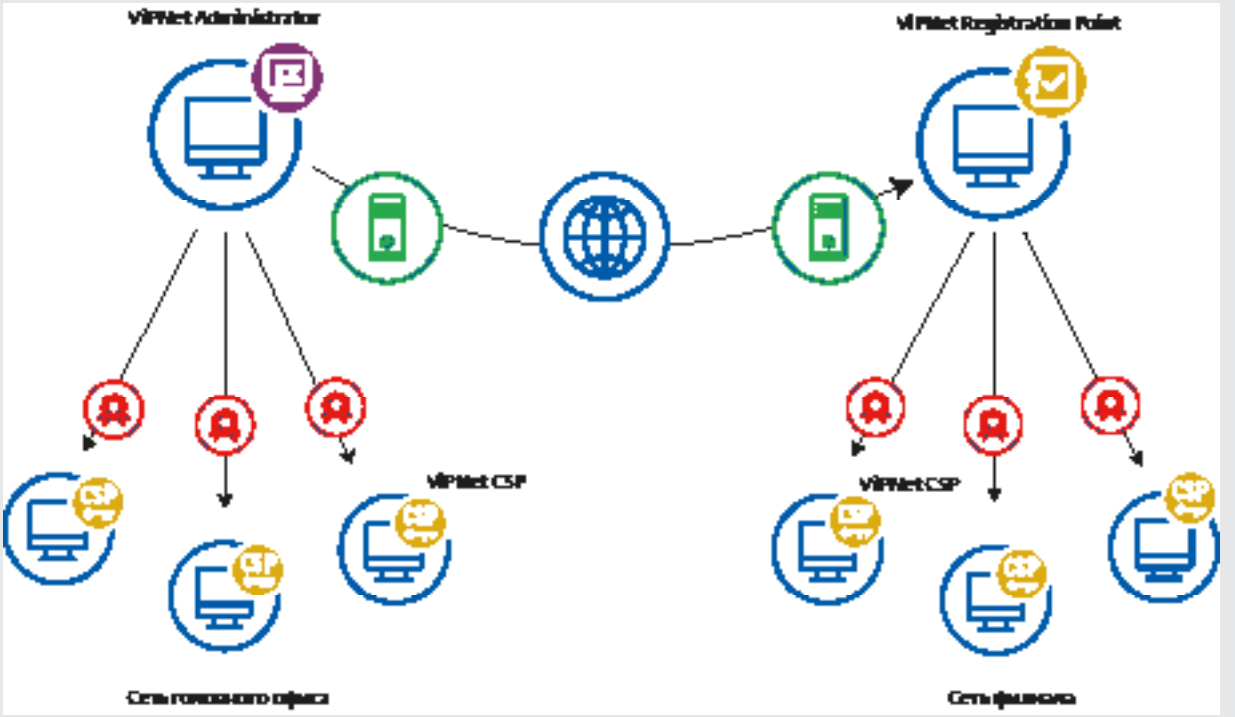

Рис.2. Сценарий использования центра регистрации

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

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].

2. Иерархическая модель доверия

Данная модель характеризуется прямой иерархией доверительных отношений. Подчиненный УЦ отправляет запрос на издание сертификата в вышестоящий УЦ. Вышестоящий центр издает сертификат и передает его обратно в подчиненный УЦ. В результате УЦ имеет сертификат, изданный по его запросу в вышестоящем УЦ. Головной УЦ при этом имеет только самоподписанный корневой сертификат [4].

Подчиненные УЦ могут выпускать сертификаты для центров, находящихся ниже 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.

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.

4. "Мостовая" модель доверия

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" центр может взаимодействовать с любым УЦ сети.

Например, удостоверяющий центр на базе программного обеспечения ViPNet поддерживает все перечисленные архитектуры и может выполнять 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 центры.

5. Браузерная модель доверия

Данная модель базируется на популярных браузерах, используемых как средство навигации в интернете. Она 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 – 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.

Выбор той или иной модели доверия осуществляется организацией исходя из ее потребностей и условий. Кроме того, разные модели доверия требуют разных затрат на реализацию и поддержку инфраструктуры. Получают широкое распространение гибридные варианты использования моделей доверия и элементов PKI в ИТ-инфраструктуре предприятия, с целью повышения защищенности отдельных бизнес-процессов и информационных систем.

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: издания сертификатов ключей проверки ЭП, поддержания инфраструктуры ключей проверки ЭП. Конечно, есть 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 основ 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 счет применения механизмов ЭП, повышение безопасности информационных ресурсов и процессов их обработки путем использования криптографических средств и сервисов PKI.

ЛИТЕРАТУРА

1. Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи".
2. **Вышенский С.В.**, **Григорьев П.В.**, **Дубенская Ю.Ю.** Инфраструктура открытых ключей с комплементарной криптографией // Вестник связи. 2007. № 9.
3. **Королев В.И.** Архитектурное построение инфраструктуры открытых ключей интегрированного информационного пространства // Безопасность информационных технологий. 2015. Т. 22. № 3. С. 59–71.
4. **Мельников Д.А.** Модель доверия для цифровой экономики Российской Федерации // Безопасность информационных технологий. 2020. Т. 27. № 2. С. 47–64.

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. Конфиден. 2002. № 6.
7. **Полянская О.Ю.**, **Горбатов В.С.** Инфраструктуры открытых ключей. М.: Просвещение, 2013. 368 с.
8. **Сабанов А.Г.** Аутентификация как составляющая единого пространства доверия // Электросвязь. 2012. № 8. С. 20–24.
9. **Сабанов А.Г.** Об уровнях доверия к первичной идентификации // Методы и технические средства 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. – 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 [Электронный ресурс]. 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 [Электронный ресурс]. URL: https://www.researchandmarkets.com/reports/5514882/global-public-key-infrastructure-pki-market (дата обращения: 06.09.2024).
16. Secure Electronic Transaction Specification. The Business Description. [Электронный ресурс]. 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 [Электронный ресурс]. URL: https://www.investopedia.com/terms/s/secure-electronic-transaction-set.asp (дата обращения: 04.09.2024).
18. Decoding Secure Electronic Transactions (SET) [Электронный ресурс]. URL: juspay.in/blog/payments/decoding-secure-electronic-transactions (дата обращения: 04.09.2024).