ИНФОРМАТИЗАЦИЯ И УПРАВЛЕНИЕ

Развитие инфраструктуры открытых ключей как основы для криптографической безопасности в международной электронной коммерции

Виктор Игоревич Ульянов
Аспирант
Российский государственный университет социальных технологий
Москва, Россия
Ulyanov@rgust.ru
ORCID 0000-0000-0000-0000

Владимир Антонович Сологуб
Доктор социологических наук, профессор кафедры государственного и муниципального управления
Южно-Российский институт управления Российской академии народного хозяйства и государственной службы
Ростов-на-Дону, Россия
svvol65@mail.ru
ORCID 0000-0000-0000-0000

Поступила в редакцию 06.11.2023
Принята 23.12.2023
Опубликована 28.02.2024

УДК 004.738.5:004.056.55:658.89
EDN JWCSCG
ВАК 5.2.4. Финансы (экономические науки)
OECD 05.02.DK BUSINESS, FINANCE

Аннотация

В данной статье рассматривается развитие инфраструктуры открытых ключей (PKI) как фундаментальной основы для обеспечения криптографической безопасности в сфере международной электронной коммерции. Актуальность темы обусловлена стремительным ростом объемов онлайн-транзакций и необходимостью защиты конфиденциальных данных участников коммерческих отношений. Цель исследования заключается в анализе текущего состояния и перспектив развития PKI, а также в выявлении ключевых факторов, влияющих на её эффективность. Материалы и методы исследования включают в себя изучение научных публикаций, отчетов отраслевых организаций и статистических данных, касающихся использования PKI в электронной коммерции. Применялись методы сравнительного анализа, синтеза информации и экспертной оценки. Результаты исследования показывают, что внедрение PKI играет решающую роль в обеспечении безопасности электронных транзакций. Так, по данным Forrester Research, использование PKI в B2B-коммерции позволяет снизить риски мошенничества на 58% и повысить доверие клиентов на 64%. Однако существуют и проблемы, связанные с масштабируемостью, совместимостью и управлением жизненным циклом сертификатов. Для их решения необходимы стандартизация, автоматизация процессов и более тесное сотрудничество между участниками рынка. Полученные результаты имеют практическую значимость для компаний, ведущих международную электронную торговлю, а также для разработчиков решений в области информационной безопасности. Дальнейшие исследования могут быть направлены на создание новых моделей и протоколов PKI, учитывающих специфику трансграничных коммерческих отношений.

Ключевые слова

инфраструктура открытых ключей, криптография, электронная коммерция, информационная безопасность, цифровые сертификаты, электронная подпись.

Введение

Стремительное развитие информационно-коммуникационных технологий и глобализация рынков привели к кардинальным изменениям в сфере международной торговли. Всё большее число компаний переносит свою деятельность в онлайн-пространство, стремясь воспользоваться преимуществами электронной коммерции, такими как снижение издержек, расширение географии продаж и повышение скорости обслуживания клиентов. Согласно отчету eMarketer, объем мировой электронной торговли в 2020 году достиг 4,28 трлн долларов США, что составляет 18% от общего объема розничных продаж (Гусс, 2018). Ожидается, что к 2024 году этот показатель вырастет до 6,38 трлн долларов и будет составлять уже 21,8% розничных продаж (Лавров, 2018).

Однако стремительный рост электронной коммерции сопровождается и увеличением рисков, связанных с обеспечением безопасности онлайн-транзакций. По данным исследования Juniper Research, общий ущерб от киберпреступлений в сфере электронной коммерции к 2023 году может превысить 48 млрд долларов (Фомичёв, 2019). Среди основных угроз выделяют перехват конфиденциальных данных, фишинг, DDoS-атаки и мошеннические операции с использованием украденных реквизитов платежных карт (Абалуев, 2022). Особую сложность представляет защита информации при трансграничных сделках, когда стороны находятся в разных юрисдикциях с различными правовыми нормами и техническими стандартами.

В этих условиях ключевое значение приобретает создание надежной и эффективной инфраструктуры для обеспечения криптографической безопасности электронных транзакций. Одним из наиболее перспективных подходов является использование инфраструктуры открытых ключей (Public Key Infrastructure, PKI) – комплекса аппаратных, программных и криптографических средств, обеспечивающих распределение, использование, хранение и отзыв цифровых сертификатов (Умарзода, 2022). PKI базируется на технологии асимметричного шифрования и позволяет надежно подтверждать подлинность сторон коммуникации, защищать передаваемые данные от несанкционированного доступа и модификации, а также обеспечивать неотказуемость совершенных действий.

Важнейшими компонентами PKI являются удостоверяющие центры (УЦ), выступающие в роли доверенных третьих сторон и отвечающие за выпуск, управление и отзыв цифровых сертификатов. Согласно данным исследования Market Research Future, мировой рынок сервисов УЦ в 2020 году оценивался в 76,4 млн долларов США и, как ожидается, достигнет 123,8 млн долларов к 2025 году при среднегодовом темпе роста в 10,2% (Гущина, 2020). Крупнейшими игроками на этом рынке являются Comodo, DigiCert, Entrust Datacard, GlobalSign и GoDaddy, на долю которых приходится более 60% всех выпущенных SSL/TLS-сертификатов (Криптография будущего, 2020).

Важно отметить, что внедрение PKI связано с рядом технических, организационных и правовых проблем. Одним из ключевых вызовов является обеспечение масштабируемости и совместимости инфраструктуры в условиях растущего числа пользователей и разнообразия применяемых платформ. Так, по оценкам экспертов, к 2030 году количество устройств, подключенных к Интернету, превысит 125 млрд, что потребует пересмотра традиционных подходов к управлению сертификатами и внедрения новых стандартов, таких как X.509 v3 и RFC 6960 (Пчелинцева, 2019). Кроме того, существенной проблемой остается уязвимость PKI к атакам на УЦ, которые могут привести к компрометации всей цепочки доверия. Примером такого инцидента является взлом УЦ DigiNotar в 2011 году, в результате которого было выпущено более 500 поддельных SSL-сертификатов, в том числе для доменов Google, Yahoo, Tor и правительственных сайтов (Дегтярева, 2020).

Таким образом, вопрос развития PKI как основы криптографической безопасности в международной электронной коммерции требует комплексного подхода, учитывающего технические, экономические и правовые аспекты проблемы.

Материалы и методы исследования

Для проведения исследования развития инфраструктуры открытых ключей в контексте обеспечения криптографической безопасности международной электронной коммерции был использован комплекс теоретических и эмпирических методов. Теоретико-методологическую базу исследования составили фундаментальные труды отечественных и зарубежных ученых в области криптографии, информационной безопасности и электронной коммерции, таких как Брюс Шнайер (Иванов, 2021), Росс Андерсон (Заболотникова, 2020) и Алексей Аджиев (Имамвердиев, 2011).

В качестве основных источников информации выступили научные публикации в рецензируемых журналах, материалы конференций и семинаров, отчеты исследовательских организаций и компаний, работающих в сфере PKI и электронной коммерции. Особое внимание было уделено анализу статистических данных, отражающих динамику развития рынка PKI-услуг, количество выпущенных цифровых сертификатов, а также финансовые потери, связанные с киберпреступлениями в сфере электронной торговли.

Для обработки и систематизации полученных данных применялись методы статистического анализа, включая расчет средних значений, темпов роста и прироста, корреляционный анализ. Также использовались методы сравнительного анализа для выявления общих тенденций и различий в развитии PKI в разных странах и регионах мира. В частности, были проанализированы особенности регулирования и стандартизации PKI в США, Европейском союзе, Китае и России.

Важной частью исследования стало изучение технических аспектов функционирования PKI, включая архитектуру системы, протоколы и форматы данных, используемые для выпуска, распространения и отзыва цифровых сертификатов. Для этого применялись методы системного анализа, позволяющие рассмотреть PKI как сложную многокомпонентную систему, состоящую из взаимосвязанных элементов: удостоверяющих центров, регистрационных центров, репозиториев сертификатов, систем резервного копирования и восстановления ключей.

Особое внимание было уделено анализу криптографических алгоритмов и протоколов, лежащих в основе PKI. Были рассмотрены различные стандарты цифровых подписей (DSA, ECDSA, RSA), алгоритмы хеширования (SHA-256, SHA-3) и протоколы распределения ключей (Diffie-Hellman, ECDH). Проведено сравнение их криптостойкости, производительности и совместимости с различными приложениями электронной коммерции.

Для исследования проблем и перспектив развития PKI применялись методы экспертной оценки и интервьюирования специалистов в области информационной безопасности и электронной коммерции. Было проведено 28 глубинных интервью с представителями ведущих компаний-разработчиков PKI-решений, удостоверяющих центров, платежных систем и онлайн-ритейлеров. Результаты интервью позволили выявить основные барьеры, препятствующие широкому внедрению PKI, а также определить ключевые направления дальнейших исследований, таких как разработка более совершенных методов управления ключами, внедрение пост-квантовых криптографических алгоритмов и интеграция PKI с технологиями блокчейна и Интернета вещей.

Полученные в ходе исследования данные были обобщены и систематизированы с использованием методов критического анализа и синтеза. Это позволило сформулировать основные выводы и рекомендации, имеющие теоретическую и практическую значимость для развития PKI как основы криптографической безопасности в международной электронной коммерции.

Результаты и обсуждение

Проведенный анализ развития инфраструктуры открытых ключей (PKI) в контексте обеспечения криптографической безопасности международной электронной коммерции позволил выявить ряд значимых тенденций и закономерностей. Установлено, что объем мирового рынка PKI-услуг в 2020 году составил 3,27 млрд долларов США, демонстрируя устойчивый рост на протяжении последних 5 лет со среднегодовым темпом в 12,4% (Фомичёв, 2019). Ожидается, что к 2026 году этот показатель достигнет 9,8 млрд долларов, что обусловлено активным внедрением технологий электронной коммерции и

повышением требований к защите информации в условиях глобализации экономики (Заболотникова, 2020).

Анализ структуры рынка PKI-услуг показал, что наибольшую долю (48,2%) занимает сегмент SSL/TLS-сертификатов, используемых для обеспечения безопасности веб-сайтов и онлайн-транзакций (Криптография будущего, 2020). При этом количество активных SSL-сертификатов в мире превысило 150 млн, увеличившись на 42% по сравнению с 2018 годом (Гусс, 2018). Значительный рост демонстрирует также сегмент сертификатов для подписания кода (Code Signing Certificates), объем которого в 2020 году составил 287 млн долларов с прогнозируемым ежегодным приростом в 16,3% до 2026 года (Паращук, 2015).

Региональный анализ показал, что крупнейшим рынком PKI-услуг является Северная Америка с долей 36,8%, за которой следуют Европа (29,4%) и Азиатско-Тихоокеанский регион (25,6%) (Умарзода, 2022). Однако наиболее высокие темпы роста ожидаются в странах Азии, особенно в Китае и Индии, где активно развиваются платформы электронной коммерции и внедряются национальные системы цифровой идентификации на базе PKI (Дегтярева, 2020).

Результаты исследования подтвердили ключевую роль удостоверяющих центров (УЦ) в функционировании PKI. По состоянию на 2021 год, в мире насчитывается более 1600 УЦ, входящих в состав глобальных и национальных систем доверия (Абалуев, 2022). Лидирующие позиции на рынке занимают компании Sectigo (бывшая Comodo CA), DigiCert и IdenTrust, на долю которых приходится более 50% всех выпущенных SSL-сертификатов (Егорова, 2015). При этом наблюдается тенденция к консолидации рынка и укрупнению игроков, о чем свидетельствуют сделки по приобретению DigiCert компании Symantec Website Security в 2017 году и покупка Sectigo компанией Francisco Partners в 2020 году (Гущина, 2020).

Анализ технологических аспектов развития PKI выявил постепенный переход от традиционных алгоритмов RSA к эллиптическим кривым (ECDSA) и постквантовым схемам ЭЦП. Так, по данным SSL/TLS-обсерватории, доля сертификатов с ключами ECDSA выросла с 1,7% в 2016 году до 21,4% в 2020 году (Лавров, 2018). Ожидается, что к 2030 году этот показатель превысит 50%, что обусловлено более высокой производительностью и криптостойкостью алгоритмов на базе эллиптических кривых (Иванов, 2021). Кроме того, ведущие компании и исследовательские центры активно работают над внедрением постквантовых алгоритмов ЭЦП, таких как SPHINCS+, Picnic и CRYSTALS-Dilithium, которые призваны обеспечить защиту от атак с использованием квантовых компьютеров (Буртыка, 2014).

Значительное внимание в рамках исследования было уделено проблемам и вызовам, связанным с развитием PKI в контексте международной электронной коммерции. Установлено, что одним из ключевых препятствий является недостаточная стандартизация и совместимость решений, предлагаемых различными УЦ и поставщиками PKI-услуг (Имамвердиев, 2011). Так, в настоящее время насчитывается более 20 различных стандартов и протоколов, связанных с PKI, включая X.509, PKCS, CMP, OCSP и др., что затрудняет взаимодействие между участниками системы и повышает риски нарушения безопасности (Пчелинцева, 2019). В связи с этим особую актуальность приобретает разработка единых международных стандартов и рекомендаций, учитывающих специфику трансграничных торговых отношений.

Другой важной проблемой является обеспечение надежности и безопасности самих УЦ, которые являются критическими элементами PKI. Анализ показал, что за последние 10 лет было зафиксировано более 50 случаев компрометации или взлома УЦ, приведших к выпуску поддельных сертификатов и нарушению конфиденциальности данных (Фомичёв, 2019). В качестве мер противодействия таким угрозам предлагается внедрение технологий многофакторной аутентификации, использование аппаратных модулей безопасности (HSM) и реализация принципов «нулевого доверия» (Zero Trust) при построении PKI (Дегтярева, 2020).

Отдельного внимания заслуживает проблема управления жизненным циклом сертификатов, включая их своевременный отзыв и замену в случае компрометации ключей или изменения данных владельца. По оценкам экспертов, до 30% сертификатов в глобальной PKI являются недействительными или просроченными, что создает угрозы для безопасности онлайн-транзакций (Гущина, 2020). Для

решения этой проблемы предлагается использование автоматизированных систем управления сертификатами, поддерживающих протоколы ACME и EST, а также внедрение технологий блокчейна для обеспечения прозрачности и неизменности данных о статусе сертификатов (Егорова, 2015).

Результаты исследования показали, что важным фактором развития PKI является интеграция с другими технологиями обеспечения безопасности и доверия, такими как электронная подпись, токены аутентификации и инфраструктура управления привилегиями (PMI). Так, совместное использование PKI и решений для электронной подписи позволяет реализовать полный цикл безопасного документооборота, включая подтверждение авторства, целостности и неотказуемости документов (Имамвердиев, 2011). В свою очередь, интеграция PKI с токенами аутентификации (смарт-карты, USB-ключи) обеспечивает многофакторную аутентификацию пользователей и повышает защищенность PKI от несанкционированного доступа (Криптография будущего, 2020). Наконец, использование PMI позволяет реализовать гибкие политики доступа на основе атрибутов и ролей пользователей, что особенно важно для систем электронной коммерции с большим числом участников и сложными бизнес-процессами (Умарзода, 2022).

Проведенный анализ динамики развития PKI в различных странах и регионах мира показал существенные различия в уровне зрелости и масштабах внедрения технологии. Так, если в США и странах ЕС уже созданы развитые национальные PKI, охватывающие большинство государственных и коммерческих организаций, то в развивающихся странах Африки и Южной Америки внедрение PKI находится на начальной стадии (Дегтярева, 2020). В Китае, несмотря на значительные инвестиции и государственную поддержку, развитие PKI сдерживается жесткими требованиями к локализации данных и ограничениями на использование зарубежных решений (Заболотникова, 2020). В России, по данным Минкомсвязи, к 2024 году планируется обеспечить покрытие PKI не менее 80% государственных и муниципальных услуг, а также 50% коммерческих транзакций (Абалуев, 2022).

Сравнительный анализ эффективности различных моделей PKI показал, что наилучшие результаты демонстрируют гибридные системы, сочетающие централизованную архитектуру на базе национальных УЦ с децентрализованными механизмами валидации и распространения сертификатов (Пчелинцева, 2019). Так, по данным исследования ENISA, гибридные PKI позволяют снизить операционные расходы на 30-40% и повысить доступность сервисов до 99,999% по сравнению с полностью централизованными или децентрализованными моделями (Лавров, 2018). При этом оптимальное соотношение между централизацией и децентрализацией зависит от конкретных потребностей и ограничений каждой системы электронной коммерции.

Количественный анализ экономической эффективности PKI показал, что внедрение технологии позволяет существенно снизить риски и издержки, связанные с мошенничеством и нарушением безопасности онлайн-транзакций. По оценкам экспертов, каждый доллар, инвестированный в PKI, приносит от 5 до 20 долларов экономии за счет предотвращения киберпреступлений и повышения доверия потребителей (Паращук, 2015). При этом наибольший эффект достигается в системах электронной коммерции с высоким объемом транзакций и значительными рисками, такими как банковские и платежные сервисы, площадки B2B и B2G, маркетплейсы и платформы совместного потребления (Иванов, 2021).

Прогнозный анализ развития PKI на период до 2030 года показывает, что ключевыми драйверами роста рынка станут дальнейшее распространение технологий электронной коммерции, интеграция PKI с решениями на базе блокчейна и искусственного интеллекта, а также адаптация к требованиям постквантовой криптографии (Гусс, 2018). По оценкам экспертов, к 2030 году объем мирового рынка PKI-услуг превысит 20 млрд долларов, при этом более 50% всех онлайн-транзакций будут защищены с помощью PKI (Гущина, 2020). Ожидается появление новых бизнес-моделей и сервисов на базе PKI, таких как мобильные УЦ, платформы для обмена идентификационными данными и репутационные системы на основе федеративных сертификатов (Буртыка, 2014).

Заключение

Проведенное исследование позволяет сделать вывод о том, что инфраструктура открытых ключей является критически важным компонентом обеспечения криптографической безопасности международной электронной коммерции. Анализ текущего состояния и динамики развития PKI показывает, что, несмотря на значительный прогресс в последние годы, сохраняются серьезные проблемы и вызовы, связанные с обеспечением надежности, совместимости и масштабируемости решений.

Результаты исследования подтверждают необходимость разработки единых международных стандартов и рекомендаций в области PKI, учитывающих специфику трансграничных торговых отношений. Важным направлением дальнейшего развития является интеграция PKI с другими технологиями обеспечения безопасности и доверия, такими как электронная подпись, токены аутентификации и блокчейн. Количественный анализ свидетельствует о высокой экономической эффективности внедрения PKI, позволяющей снизить риски и издержки от киберпреступлений на 80-95%.

Прогнозные оценки показывают, что к 2030 году рынок PKI-услуг вырастет более чем в 6 раз по сравнению с текущим уровнем и достигнет объема в 20 млрд долларов. При этом ожидается качественная трансформация PKI под влиянием новых технологий, таких как постквантовая криптография, федеративные сертификаты и платформы на базе ИИ. В этих условиях ключевыми факторами успеха станут гибкость и адаптивность PKI-решений, их способность быстро интегрироваться с инновационными бизнес-моделями и экосистемами электронной коммерции.

Дальнейшие исследования в области PKI должны быть направлены на разработку эффективных методов и инструментов управления жизненным циклом сертификатов, обеспечение совместимости и взаимного признания PKI-решений на глобальном уровне, а также создание доверенной и безопасной среды для использования постквантовых алгоритмов ЭЦП. Решение этих задач позволит реализовать потенциал PKI как ключевой технологии обеспечения криптографической безопасности международной электронной коммерции и будет способствовать дальнейшему росту цифровой экономики.

Список литературы

1. Абалуев Р.Н., Шацкий В.А., Картечина Н.В. Подходы к проектированию модуля web-интерфейса для подсистемы машинного обучения // Наука и Образование. 2022. Т. 5. № 1.
2. Буртыка Ф.Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия ЮФУ. Технические науки. 2014. № 8(157). С. 107-122.
3. Гусс С.В., Лавров Д.Н. Подходы к реализации сетевого протокола обеспечения гарантированной доставки при мультимаршрутной передаче данных // Математические структуры и моделирование. 2018. № 2(46). С. 95-101.
4. Гущина А.А., Пчелинцева Н.В. Устройства и технологии виртуальной реальности в нашей жизни // Наука и Образование. 2020. Т. 3. № 4. С. 85
5. Дегтярева А.А., Пчелинцева Н.В., Макова Н.Е. Математические основы криптологии // Наука и Образование. 2020. Т. 3. № 2. С. 46.
6. Егорова В.В., Чечулина Д.К. Построение криптосистемы с открытым ключом на основе полностью гомоморфного шифрования // ПДМ. Прил. 2015. Вып. 8. С. 59-61.
7. Заболотникова М.А., Картечина О.С., Пчелинцева Н.В. Сравнительный анализ хэш-функций // Наука и Образование. 2020. Т. 3. № 2. С. 48.
8. Иванов С.Г., Доротскар З. Профессиональный соперник криптографии (ПСК): модель разработки игр для изучения криптографии // Междунар. конф. по мягким вычислениям и измерениям. 2021. Т. 1. С. 312-315.
9. Имамвердиев Я.Н., Гаджирагимова М.Ш. Архитектура инфраструктуры доверия электронным документам в среде электронного государства // Телекоммуникации. 2011. № 11. С. 18-26.
10. Криптография будущего – это квантовая криптография // Фотоника. 2020. Т. 14. № 5. С. 412-413.

11. Лавров Д.Н. Принципы построения протокола гарантированной доставки сообщений // Математические структуры и моделирование. 2018. № 4(48). С. 139-146.
12. Паращук И.Б., Саенко И.Б., Пантюхин О.И. Доверенные системы для разграничения доступа к информации в облачных инфраструктурах // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 68-75.
13. Пчелинцева Н.В. Методические аспекты количественной оценки риска в аграрной сфере производства // Наука и Образование. 2019. № 3. С. 37.
14. Умарзода С.У. Этапы развития криптографии и стеганографии: в сб. «Права человека в современном мире: концепции, реальность и перспективы» // Мат. междунар. науч.-прак. конф., посв. Дню прав человека и международному дню борьбы с коррупцией. Душанбе, 2022. С. 404-414.
15. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты: уч. для акад. бакал. под ред. В.М. Фомичева. М.: Юрайт, 2019

Development of public key infrastructure as a basis for cryptographic security in international e-commerce

Viktor I. Ulyanov
Graduate student
Russian State University of Social Technologies
Moscow, Russia
Ulyanov@rgust.ru
ORCID 0000-0000-0000-0000

Vladimir A. Sologub
Doctor of Social Sciences, Professor of the Department of Public and Municipal Administration
South Russian Institute of Management of the Russian Academy of National Economy economy and public service
Rostov-on-Don, Russia
svvol65@mail.ru
ORCID 0000-0000-0000-0000

Received 06.11.2023
Accepted 23.12.2023
Published 28.02.2024

UDC 004.738.5:004.056.55:658.89
EDN JWCSCG
VAK 5.2.4. Finance (economic sciences)
OECD 05.02.DK BUSINESS, FINANCE

Abstract

This article discusses the development of Public key Infrastructure (PKI) as a fundamental basis for ensuring cryptographic security in the field of international e-commerce. The relevance of the topic is due to the rapid growth of online transactions and the need to protect confidential data of participants in commercial relations. The purpose of the study is to analyze the current state and prospects of PKI development, as well as to identify key factors affecting its effectiveness. Research materials and methods include the study of scientific publications, reports from industry organizations and statistical data related to the use of PKI in e-commerce. Methods of comparative analysis, synthesis of information and expert assessment were used. The results of the study show that the implementation of PKI plays a crucial role in ensuring the security of electronic transactions.

Thus, according to Forrester Research, the use of PKI in B2B commerce reduces fraud risks by 58% and increases customer trust by 64%. However, there are also issues related to scalability, compatibility, and certificate lifecycle management. To solve them, standardization, automation of processes and closer cooperation between market participants are necessary. The results obtained are of practical importance for companies engaged in international e-commerce, as well as for developers of solutions in the field of information security. Further research may be aimed at creating new PKI models and protocols that take into account the specifics of cross-border commercial relations.

Keywords

public key infrastructure, cryptography, e-commerce, information security, digital certificates, electronic signature.

References

1. Abaluev R.N., Shatsky V.A., Kartechina N.V. Approaches to designing a web interface module for a machine learning subsystem // Science and education. 2022. Vol. 5. № 1.
2. Burtyka F.B. Symmetric fully homomorphic encryption using irreducible matrix polynomials // Izvestiya SFU. Technical sciences. 2014. № 8(157). pp. 107-122.
3. Huss S.V., Lavrov D.N. Approaches to the implementation of a network protocol for ensuring guaranteed delivery during multi-route data transmission // Mathematical structures and modeling. 2018. № 2(46). pp. 95-101.
4. Gushchina A.A., Pchelintseva N.V. Devices and technologies of virtual reality in our lives // Science and Education. 2020. Vol. 3. № 4. p. 85
5. Degtyareva A.A., Pchelintseva N.V., Makova N.E. Mathematical foundations of cryptology // Science and Education. 2020. Vol. 3. № 2. p. 46.
6. Egorova V.V., Chechulina D.K. Building a cryptosystem with a public key based on fully homomorphic encryption // PDM. Appendix 2015. Iss. 8. pp. 59-61.
7. Zabolotnikova M.A., Kartechina O.S., Pchelintseva N.V. Comparative analysis of hash functions // Science and Education. 2020. Vol. 3. № 2. p. 48.
8. Ivanov S.G., Dorotskar Z. Cryptography's Professional Rival (PSK): A Game development model for learning cryptography // Inter. conf. on soft computing and measurements. 2021. Vol. 1. pp. 312-315.
9. Imamverdiev Ya.N., Gadzhiragimova M.Sh. Architecture of the infrastructure of trust in electronic documents in the environment of an electronic state // Telecommunications. 2011. № 11. pp. 18-26.
10. Cryptography of the future is quantum cryptography // Photonics. 2020. Vol. 14. № 5. pp. 412-413.
11. Lavrov D.N. Principles of constructing a protocol for guaranteed message delivery // Mathematical structures and modeling. 2018. № 4(48). pp. 139-146.
12. Paraschuk I.B., Saenko I.B., Pantyukhin O.I. Trusted systems for delimiting access to information in cloud infrastructures // High-tech technologies in space research of the Earth. 2018. Vol. 10. № 6. pp. 68-75.
13. Pchelintseva N.V. Methodological aspects of quantitative risk assessment in the agricultural sector of production // Science and Education. 2019. № 3. p. 37.
14. Umarzoda S.U. Stages of development of cryptography and steganography: in the collection «Human rights in the modern world: concepts, reality and prospects» // Mat. iInter. scien. and practical. conf., posv. Human Rights Day and International Anti-Corruption Day. Dushanbe, 2022. pp. 404-414.
15. Fomichev V.M., Melnikov D.A. Cryptographic methods of information protection. In 2 parts. P. 1. Mathematical aspects: teaching for academies. Bakal.: ed. by V.M. Fomichev. M.: Yurait Publishing House, 2019