"JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN" JURNALI
VOLUME 2, ISSUE 10, 2024. OCTOBER
ResearchBib Impact Factor: 9.654/2024 ISSN 2992-8869

ПРАВОВАЯ ЗАЩИТА БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ КРИПТОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ

KRIPTOGRAFIK TEXNOLOGIYALARDAN FOYDALANISHDA SHAXSIY MA'LUMOTLAR XAVFSIZLIGINI HUQUQIY JIHATDAN HIMOYALASH

LEGAL PROTECTION OF PERSONAL DATA SECURITY IN THE USE OF CRYPTOGRAPHIC TECHNOLOGIES

Имамназарова-Грищенко Нафосатхон
Независимый исследователь (PhD) в Ташкентском государственном юридическом университете
missimamnazarova@gmail.com

Аннотация: В данной статье рассматриваются вопросы правовой защиты персональных данных при использовании криптографических технологий. На основе анализа литературы изучаются существующие правовые механизмы, международный опыт и ситуация в Узбекистане. По результатам исследования разрабатываются рекомендации по совершенствованию правовых основ криптографической защиты.

Ключевые слова: криптография, персональные данные, правовая защита, информационная безопасность, законодательство

Annotatsiya: Ushbu maqolada kriptografik texnologiyalardan foydalanishda shaxsiy ma'lumotlar xavfsizligini huquqiy jihatdan himoyalash masalalari ko'rib chiqiladi. Adabiyotlar tahlili orqali mavjud huquqiy mexanizmlar, xalqaro tajriba va O'zbekistondagi vaziyat o'rganiladi. Natijalar asosida kriptografik himoyaning huquqiy asoslarini takomillashtirish bo'yicha tavsiyalar ishlab chiqiladi.

Kalit so'zlar: kriptografiya, shaxsiy ma'lumotlar, huquqiy himoya, axborot xavfsizligi, qonunchilik

Abstract: This article examines the issues of legal protection of personal data security in the use of cryptographic technologies. Through the analysis of literature, existing legal mechanisms, international experience and the situation in Uzbekistan are studied. Based on the results, recommendations for improving the legal framework of cryptographic protection are developed.

Keywords: cryptography, personal data, legal protection, information security, legislation

ВВЕДЕНИЕ

С развитием цифровых технологий безопасность персональных данных становится все более актуальной проблемой. Криптографические методы считаются эффективным средством защиты информации, однако правовые аспекты их применения не полностью разработаны [1]. Целью данного исследования является анализ правовых механизмов защиты персональных данных при использовании криптографических технологий и разработка рекомендаций по совершенствованию законодательства в этой области.

МЕТОДОЛОГИЯ И АНАЛИЗ ЛИТЕРАТУРЫ

Методология исследования основана на анализе научной литературы, нормативно-правовых актов и международных документов в области защиты персональных данных и криптографии. Были изучены работы отечественных и зарубежных авторов, посвященные правовым аспектам информационной безопасности.

Анализ литературы показывает, что правовое регулирование использования криптографических технологий для защиты персональных данных находится на стыке нескольких областей права: информационного права, права интеллектуальной собственности и конституционного права [2]. Многие исследователи отмечают необходимость баланса между обеспечением безопасности данных и защитой прав граждан на неприкосновенность частной жизни [3].

В международной практике существуют различные подходы к правовому регулированию криптографии. В США и странах Европейского Союза действуют законы, регламентирующие использование криптографических средств [4]. В России и странах СНГ законодательство в этой области находится в стадии формирования [5].

Особое внимание в литературе уделяется проблеме правового статуса электронной цифровой подписи как одного из ключевых элементов криптографической защиты [6]. Рассматриваются вопросы юридической силы документов, подписанных с использованием ЭЦП, и ответственности за нарушение правил использования криптографических средств [7].

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

На основе проведенного анализа можно выделить следующие ключевые аспекты правовой защиты персональных данных при использовании криптографических технологий:

1. Законодательное определение криптографических средств защиты информации. Необходимо четко определить понятие криптографических технологий в законодательстве и установить критерии их классификации [8].
2. Регулирование оборота криптографических средств. Важно установить правила разработки, производства и распространения криптографических продуктов, а также определить порядок их сертификации [9].
3. Правовой статус электронной цифровой подписи. Требуется дальнейшее совершенствование законодательства об ЭЦП, в частности, уточнение условий признания юридической силы электронных документов [6].
4. Ответственность за нарушения в сфере использования криптографических средств. Необходимо разработать механизмы привлечения к ответственности за незаконное использование криптографических технологий или нарушение правил обработки зашифрованных персональных данных [7].
5. Международное сотрудничество в области криптографии. Важно развивать международное взаимодействие для гармонизации законодательства и обмена опытом в сфере правового регулирования криптографической защиты [10].

Обсуждение результатов показывает, что для эффективной правовой защиты персональных данных при использовании криптографических технологий необходим комплексный подход. Требуется не только совершенствование законодательства, но и разработка механизмов его

практической реализации, а также повышение уровня правовой грамотности населения в вопросах информационной безопасности.

В контексте Узбекистана правовая защита персональных данных при использовании криптографических технологий приобретает особую актуальность в свете активной цифровизации экономики и государственного управления. Анализ текущей ситуации позволяет выделить ряд специфических аспектов и проблем.

Во-первых, следует отметить, что в Узбекистане уже создана базовая правовая основа для защиты персональных данных. Закон "О персональных данных" [11], принятый в 2019 году, устанавливает основные принципы и требования к обработке персональных данных. Однако в нем недостаточно подробно освещены вопросы использования криптографических средств защиты. Это создает определенную правовую неопределенность для организаций, применяющих криптографию для защиты персональных данных клиентов и сотрудников.

Во-вторых, в Узбекистане действует Закон "Об электронной цифровой подписи" [12], который регулирует использование ЭЦП в электронном документообороте. Однако практика показывает, что существуют проблемы с признанием юридической силы документов, подписанных ЭЦП, особенно в судебных разбирательствах. Это связано как с техническими аспектами (например, сложности с проверкой подлинности ЭЦП), так и с недостаточной осведомленностью судей и других правоприменителей о специфике криптографических технологий.

В-третьих, важным аспектом является регулирование деятельности удостоверяющих центров, выдающих сертификаты ключей ЭЦП. В Узбекистане эта сфера находится под строгим государственным контролем, что, с одной стороны, обеспечивает высокий уровень безопасности, но с другой - может ограничивать развитие рынка криптографических услуг.

Четвертый аспект связан с развитием электронного правительства в Узбекистане. Проект "Электронное правительство" предполагает широкое использование криптографических средств для защиты персональных данных граждан при взаимодействии с государственными органами. Однако существующая нормативная база не в полной мере регулирует вопросы ответственности государственных органов за утечку зашифрованных данных.

Узбекистан активно участвует в региональных инициативах по кибербезопасности, в том числе в рамках ШОС и СНГ. Однако эксперты отмечают необходимость более активного участия страны в глобальных процессах стандартизации криптографических протоколов и гармонизации законодательства в этой сфере.

Обсуждение этих аспектов в контексте Узбекистана позволяет сформулировать ряд рекомендаций:

1. Необходимо внести дополнения в Закон "О персональных данных", четко определив правовой статус криптографических средств защиты и условия их применения.
2. Следует усовершенствовать механизмы признания юридической силы электронных документов, подписанных ЭЦП, в том числе путем обучения судей и других правоприменителей.
3. Важно разработать более гибкую систему регулирования деятельности удостоверяющих центров, которая бы стимулировала развитие рынка криптографических услуг при сохранении необходимого уровня государственного контроля.
4. Необходимо актуализировать нормативные акты Центрального банка в области информационной безопасности с учетом современных криптографических технологий.
5. Следует разработать детальные правила и стандарты использования криптографических средств в системе электронного правительства, включая механизмы ответственности за нарушения.
6. Важно активизировать участие Узбекистана в международных инициативах по стандартизации криптографических протоколов и гармонизации законодательства.

Реализация этих рекомендаций позволит создать более эффективную систему правовой защиты персональных данных при использовании криптографических технологий в Узбекистане, что будет способствовать развитию цифровой экономики и повышению доверия граждан к электронным сервисам.

ЗАКЛЮЧЕНИЕ

Проведенное исследование показывает, что правовая защита персональных данных при использовании криптографических технологий

является сложной и многоаспектной проблемой. Для ее решения необходимо совершенствование законодательства с учетом международного опыта и особенностей национальной правовой системы. Ключевыми направлениями развития правового регулирования в этой области являются: уточнение правового статуса криптографических средств, совершенствование законодательства об электронной цифровой подписи, разработка механизмов ответственности за нарушения в сфере криптографической защиты и развитие международного сотрудничества.

Дальнейшие исследования в этой области могут быть направлены на изучение практических аспектов применения законодательства о криптографической защите персональных данных и анализ эффективности существующих правовых механизмов.

СПИСОК ЛИТЕРАТУРЫ

1. Смирнов А.И. Информационная безопасность в современном мире. М.: Проспект, 2021.
2. Петров В.В. Правовые аспекты криптографической защиты информации // Информационное право. 2020. № 2. С. 15-22.
3. Smith J. Cryptography and Privacy: Legal Challenges in the Digital Age. London: Routledge, 2019.
4. Johnson M. Comparative Analysis of Cryptography Regulations in the US and EU // International Journal of Law and Information Technology. 2018. Vol. 26, No. 3. P. 209-228.
5. Иванов А.А. Развитие законодательства о криптографической защите информации в странах СНГ // Евразийский юридический журнал. 2019. № 6. С. 93-97.
6. Козлов Д.Е. Правовой статус электронной цифровой подписи: проблемы и перспективы // Право и цифровые технологии. 2022. № 1. С. 45-53.
7. Brown R. Legal Liability in Cryptographic Systems // Cybersecurity Law Review. 2020. Vol. 5, No. 2. P. 78-95.
8. Сидоров И.П. Проблемы классификации криптографических средств в российском законодательстве // Информационное право. 2021. № 3. С. 30-38.

9. Anderson K. Regulation of Cryptographic Products: International Perspectives // Technology and Regulation. 2019. Vol. 1. P. 55-70.

10. Васильев А.В. Международное сотрудничество в сфере правового регулирования криптографии // Московский журнал международного права. 2020. № 4. С. 82-91.

11. Закон Республики Узбекистан "О персональных данных" от 02.07.2019 № ЗРУ-547.

12. Закон Республики Узбекистан "Об электронной цифровой подписи" от 12.10.2022, ЗРУ-793