УДК 33 **DOI: 10.34670/AR.2026.42.70.050**

Экономический аспект использования конечных полей Галуа в защите информации

Грушицын Александр Степанович

Преподаватель кафедры информационной безопасности,
Университет «Синергия»,
125190, Российская Федерация, Москва, Ленинградский просп., 80, корп. Г;
e-mail: nicifor@bk.ru

Аннотация

В статье исследуется трансформация информационной безопасности из сугубо технической задачи в фундаментальный экономический фактор в условиях цифровизации глобальной экономики. Основное внимание уделяется роли криптографии на основе конечных полей Галуа как математического фундамента, обеспечивающего надежность и доверие в цифровых системах. Анализируется прямое экономическое значение криптографических алгоритмов для защиты финансовых транзакций, обеспечения целостности данных и работы асимметричной криптографии, поддерживающей такие сферы, как электронная коммерция и цифровое государственное управление. Отдельно рассматривается возникновение новой макроэкономической угрозы, связанной с развитием квантовых вычислений, которые ставят под сомнение стойкость современных криптосистем. В статье обосновывается, что переход на постквантовую криптографию представляет собой масштабный экономический процесс, требующий значительных инвестиций, международной координации и пересмотра стратегий управления рисками. Делается вывод о необходимости интеграции криптографической повестки в экономическое планирование и государственную политику для обеспечения долгосрочной устойчивости и конкурентоспособности в цифровую эпоху. Работа подчеркивает, что управление криптографическими рисками и инвестиции в соответствующие исследования становятся критическим элементом экономической стратегии государства и бизнеса, напрямую влияющим на технологический суверенитет и устойчивость критической инфраструктуры.

Для цитирования в научных исследованиях

Грушицын А.С. Экономический аспект использования конечных полей Галуа в защите информации // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 12А. С. 611-617. DOI: 10.34670/AR.2026.42.70.050

Ключевые слова

информационная безопасность, цифровая экономика, конечные поля Галуа, криптография, экономический фактор, квантовые вычисления, постквантовая криптография, киберриски, инвестиции в безопасность, технологический суверенитет, критическая инфраструктура.

Введение

В условиях всеобъемлющей цифровой трансформации глобальной экономики информационная безопасность перестала быть узкоспециальной технической дисциплиной и эволюционировала в стратегический экономический актив, непосредственно влияющий на финансовую стабильность, конкурентные преимущества и национальный суверенитет. Надежная защита цифровых данных и коммуникаций превратилась в критическую инфраструктуру, краеугольный камень, на котором держится функционирование международных финансовых систем, электронной коммерции, глобальных цепочек поставок и цифрового государственного управления. Парадоксально, но основу этой защиты, оцениваемой триллионами долларов, составляют глубокие математические абстракции, среди которых центральное место занимает теория конечных полей, или полей Галуа. Эти алгебраические структуры, обеспечивая криптографическую стойкость, создают экономическую ценность, формируя доверие — ключевой нематериальный актив цифровой экономики. Таким образом, понимание взаимосвязи между математическими алгоритмами и экономическими последствиями их надежности становится императивом не только для инженеров, но и для экономистов, стратегов корпоративного уровня и государственных политиков, ответственных за формирование регуляторной и инвестиционной среды.

Основная часть

Конечные поля Галуа представляют собой математические системы с конечным числом элементов, в которых определены и корректно выполняются все основные арифметические операции — сложение, вычитание, умножение и деление (на ненулевой элемент), подчиняющиеся классическим законам ассоциативности, коммутативности и дистрибутивности. Простейшим примером является поле из двух элементов (0 и 1), образующее фундамент битовых операций. Однако для практического применения в криптографии особенно важны расширенные поля, такие как $GF(2^8)$, состоящее из 256 элементов, которое можно интерпретировать как поле байтов. Именно в таких структурах выполняются преобразования, лежащие в основе современных стандартов шифрования. Экономическая значимость этих абстрактных конструкций проявляется в их способности эффективно и безопасно реализовывать криптографические протоколы, которые защищают цифровые активы и транзакции. Эффективность операций в конечных полях позволяет осуществлять шифрование и проверку целостности данных с высокой скоростью, что является техническим условием для экономической целесообразности массовых цифровых операций, от микроплатежей до высокочастотного трейдинга.

Прямое экономическое значение криптографии на конечных полях можно проследить в нескольких ключевых секторах цифровой экономики. В сфере защиты финансовых транзакций симметричные алгоритмы, такие как Advanced Encryption Standard (AES), фундаментально опирающиеся на арифметику в поле $GF(2^8)$, обеспечивают безопасность каждой операции с банковской картой, денежного перевода или биржевой сделки. Надежность этого шифра является экономическим буфером, предотвращающим колоссальные убытки от мошенничества и несанкционированного доступа. Нарушение AES привело бы не только к прямым хищениям средств, но и к эрозии доверия к платежным системам, что могло бы спровоцировать системный

кризис ликвидности и снижение потребительской активности. Доверие, обеспеченное криптографией, таким образом, трансформируется в экономическую стабильность и снижение транзакционных издержек.

Другим критически важным применением является обеспечение целостности и доступности данных. Коды коррекции ошибок, в частности коды Рида-Соломона, основанные на вычислениях в GF(256), широко внедрены в системы хранения информации (жесткие диски, RAID-массивы, SSD-накопители) и каналы передачи данных (от оптических носителей до стандартов мобильной связи 5G и спутниковой коммуникации). Их способность автоматически обнаруживать и исправлять ошибки напрямую влияет на отказоустойчивость и надежность критической цифровой инфраструктуры. Экономический эффект здесь выражается в предотвращении простоев и потерь данных. Сбой в крупном центре обработки данных из-за некорректируемых ошибок может обойтись компании в миллионы долларов в час не только в виде прямых убытков от простоя, но и вследствие репутационного ущерба, судебных издержек и штрафов за несоответствие регуляторным требованиям. Таким образом, математические алгоритмы на полях Галуа выполняют функцию экономического страхования, минимизируя операционные риски.

В области асимметричной криптографии, хотя такие широко распространенные алгоритмы, как RSA (Rivest–Shamir–Adleman), и основываются на теории чисел и сложности факторизации больших целых чисел, они концептуально связаны с более общими алгебраическими структурами, включая конечные поля. Эти системы составляют основу для установления защищенных соединений по протоколу HTTPS, цифровых подписей для электронных контрактов и надежной аутентификации пользователей. Их устойчивость поддерживает весь объем глобальной электронной коммерции, который, по различным оценкам, достиг нескольких триллионов долларов США в год. Надежность RSA и подобных алгоритмов гарантирует, что сделки, заключаемые онлайн, являются юридически значимыми и защищенными от подделки. Любое ослабление криптографической стойкости этих систем напрямую угрожает экономической основе целых отраслей, таких как дистанционная торговля, финтех и цифровые государственные услуги, потенциально вызывая сокращение рынков и рост страховых премий на киберриски.

Однако устойчивость этой экономико-криптографической парадигмы столкнулась с беспрецедентным вызовом — прогрессом в области квантовых вычислений. Появление достаточно мощного квантового компьютера представляет собой, возможно, одну из самых серьезных системных экономических угроз XXI века. Квантовые алгоритмы, в частности алгоритм Шора, теоретически способны решать за полиномиальное время именно те математические задачи (факторизацию больших чисел и вычисление дискретного логарифма), на сложности которых базируется стойкость большинства современных асимметричных криптосистем. Экономические последствия реализации такой угрозы трудно переоценить. Под угрозой оказалась бы не только будущая, но и вся историческая зашифрованная информация, защищенная уязвимыми алгоритмами. Это включает архивы государственной и военной тайны, коммерческую интеллектуальную собственность, базы персональных данных миллиардов граждан, а также активы в криптовалютах. Экономический ущерб от одномоментной девальвации конфиденциальности и целостности цифровой информации мог бы привести к глубокому системному кризису доверия, коллапсу отдельных сегментов финансового рынка и геополитической дестабилизации.

Парадоксальным образом, квантовая угроза сама по себе формирует новый стремительно растущий рынок — рынок квантовых технологий и постквантовой криптографии. Инвестиции в эти области со стороны государств и корпораций носят превентивный экономический характер. Страны и компании, которые первыми овладеют устойчивыми к квантовым атакам технологиями и стандартами, получат колоссальное конкурентное преимущество и усилят свой технологический суверенитет. Экономическая необходимость перехода всей глобальной цифровой инфраструктуры на постквантовые криптографические алгоритмы создает масштабную инвестиционную повестку. Этот процесс потребует многолетних усилий и капиталовложений, оцениваемых в десятки миллиардов долларов, на обновление программно-аппаратных комплексов: операционных систем, сетевого оборудования, микросхем аппаратной защиты (HSM), программных библиотек и протоколов связи. Затраты будут включать не только прямые инвестиции в разработку и внедрение, но и косвенные издержки, связанные с тестированием, сертификацией, обучением персонала и обеспечением обратной совместимости. Координация этого перехода между государственным и частным секторами становится задачей макроэкономического масштаба, сравнимой с модернизацией критической инфраструктуры.

В контексте постквантового перехода конечные поля Галуа не утрачивают своей актуальности, а демонстрируют адаптивность как математический инструмент. Многие многообещающие кандидаты в алгоритмы постквантовой криптографии, например, некоторые схемы на основе решеток (lattice-based cryptography) и многомерных квадратичных систем, активно используют сложные алгебраические конструкции, включая расширения полей Галуа. Это свидетельствует о том, что данные математические структуры остаются фундаментальным языком, на котором описывается безопасность. Инвестиции в исследования и разработку таких алгоритмов — это, по сути, инвестиции в долгосрочную экономическую безопасность. Компании, которые уже сейчас начинают процесс криптографической агностики, внедряя гибкие, обновляемые решения и изучая постквантовые кандидаты, формируют экономическую устойчивость, снижая будущие риски и избегая катастрофических затрат в момент неизбежного принудительного перехода. Это стимулирует формирование нового сектора экономики, включающего специализированные стартапы, консалтинговые агентства по кибербезопасности и производителей защищенного оборудования.

Ключевую роль в управлении этим глобальным экономическим риском и формировании нового рынка играет государственная политика и международная стандартизация. Органы по стандартизации, такие как Национальный институт стандартов и технологий (NIST) США, ведут многолетнюю открытую работу по отбору и стандартизации постквантовых криптографических алгоритмов. Эта деятельность имеет прямое экономическое измерение: единые, проверенные международным сообществом стандарты снижают издержки внедрения для бизнеса, предотвращают фрагментацию рынка и создают предсказуемые условия для инвестиций. Для национальных государств поддержка и ускорение перехода на постквантовую криптографию становится элементом обеспечения экономической безопасности и защиты критической инфраструктуры (энергосистем, транспортных сетей, систем здравоохранения) от потенциального шантажа или диверсионных атак с использованием квантовых возможностей противника. Таким образом, криптографическая политика трансформируется в инструмент экономической и геополитической конкуренции.

Конечные поля Галуа и основанная на них криптография представляют собой не абстрактную математическую теорию, а фундаментальный экономический инструмент, обеспечивающий ценность и стабильность цифровой экономики. Они создают технические

условия для снижения транзакционных издержек, защиты активов и поддержания доверия в виртуальной среде. Надвигающаяся квантовая революция, несущая угрозу этому устоявшемуся порядку, одновременно формирует новую экономическую реальность, требующую масштабных превентивных инвестиций, международной координации и переосмысления подходов к долгосрочному планированию в области кибербезопасности. Успешное управление этим переходом определит распределение экономических преимуществ и рисков в цифровую эпоху, сделав глубокое понимание взаимосвязи математики, технологий и экономики критически важным компетенцией для лиц, принимающих стратегические решения на всех уровнях.

Заключение

В эпоху тотальной цифровизации экономических процессов информационная безопасность окончательно трансформировалась из технической проблемы в системный экономический фактор, определяющий устойчивость финансовых рынков, целостность глобальных цепочек поставок и доверие к институтам государственного управления. Как продемонстрировано в данном исследовании, абстрактные математические структуры — конечные поля Галуа — выступают краеугольным камнем этой безопасности, обеспечивая криптографическую стойкость, которая напрямую конвертируется в экономическую ценность. Эффективные алгоритмы шифрования и контроля целостности данных, основанные на арифметике в полях Галуа, минимизируют операционные и репутационные риски, снижают транзакционные издержки и создают необходимые условия для существования многотриллионных рынков электронной коммерции и цифровых финансов.

Стабильность этой модели оказалась под фундаментальной угрозой в связи с прогрессом квантовых вычислений. Способность квантового компьютера потенциально взломать используемые сегодня асимметричные криптосистемы представляет собой беспрецедентный макроэкономический риск, угрожающий девальвировать конфиденциальность и целостность всей накопленной цифровой информации. Это потребует глобального и крайне затратного перехода на постквантовые криптографические стандарты, который уже сейчас формирует новую инвестиционную повестку и рынок специализированных решений. Данный переход следует рассматривать не как исключительно технологическую задачу, а как сложный экономический процесс, требующий долгосрочных капиталовложений, скоординированных действий между государственным и частным сектором и выработки четких международных стандартов.

Обеспечение цифровой безопасности на основе передовых математических методов, включая как классические, так и постквантовые алгоритмы, перестает быть уделом исключительно ИТ-специалистов. Оно становится стратегическим императивом для экономистов, корпоративных стратегов и политиков, ответственных за устойчивый рост и конкурентоспособность в XXI веке. Страны и компании, которые смогут наиболее эффективно управлять криптографическими рисками и инвестировать в инфраструктуру будущего, получат решающее преимущество в обеспечении своей экономической безопасности и технологического суверенитета. Следовательно, дальнейшие исследования и практические усилия должны быть сосредоточены на комплексной оценке экономических последствий криптографических переходов, разработке адаптивных регуляторных моделей и стимулировании инноваций, которые позволят превратить надвигающиеся вызовы в источники новой устойчивости и экономических возможностей.

Библиография

1. М. В. Ступина «Разработка подхода к обеспечению информационной безопасности в веб-ориентированных информационных системах при передаче данных с использованием интерфейса Web Cryptography API», Известия Кабардино-Балкарского научного центра РАН Том 26 № 1 2024
2. Таранников Ю. В. «Самокорректирующиеся коды и их применения в криптографии», 2023, МГУ
3. Э.Джонстон «Программирование квантовых компьютеров», Питер, 2021
4. Bardis N. G. et al. Fast implementation zero knowledge identification schemes using the Galois Fields arithmetic //2012 IX International Symposium on Telecommunications (BIHTEL). – IEEE, 2012. – С. 1-6.
5. Davletova A. et al. Enhancing Cryptographic System Security based on Finite Fields //2024 14th International Conference on Advanced Computer Information Technologies (ACIT). – IEEE, 2024. – С. 476-480.
6. George K., Michaels A. J. Designing a block cipher in Galois extension fields for IoT security //IoT. – 2021. – Т. 2. – №. 4. – С. 669-687.
7. Hazzazi M. M. et al. A novel cipher-based data encryption with galois field theory //Sensors. – 2023. – Т. 23. – №. 6. – С. 3287.
8. L. N. Chang "Quantum Systems based upon Galois Fields — from Sub-quantum to Super-quantum Correlations", Virginia Tech, 2014
9. Nardo L. G. et al. A reliable chaos-based cryptography using Galois field //Chaos: An Interdisciplinary Journal of Nonlinear Science. – 2021. – Т. 31. – №. 9.
10. Zhang Y. et al. The probabilistic image encryption algorithm based on galois field GF (257) //IETE Journal of Research. – 2024. – Т. 70. – №. 7. – С. 6286-6299.

The Economic Aspect of Using Galois Finite Fields in Information Security

Aleksandr S. Grushitsyn

Lecturer, Department of Information Security,
Synergy University,
125190, 80, Leningradsky ave., bldg. G, Moscow, Russian Federation;
e-mail: nicifor@bk.ru

Abstract

The article investigates the transformation of information security from a purely technical task into a fundamental economic factor in the conditions of the digitalization of the global economy. Primary focus is given to the role of cryptography based on Galois finite fields as the mathematical foundation ensuring reliability and trust in digital systems. The direct economic significance of cryptographic algorithms for protecting financial transactions, ensuring data integrity, and the operation of asymmetric cryptography supporting spheres such as e-commerce and digital public administration is analyzed. The emergence of a new macroeconomic threat related to the development of quantum computing, which calls into question the resilience of modern cryptosystems, is separately considered. The article substantiates that the transition to post-quantum cryptography represents a large-scale economic process requiring significant investments, international coordination, and a revision of risk management strategies. The conclusion is drawn about the necessity of integrating the cryptographic agenda into economic planning and state policy to ensure long-term sustainability and competitiveness in the digital era. The work emphasizes that managing cryptographic risks and investing in related research are becoming critical elements of the economic strategy of the state and business, directly impacting technological sovereignty and the resilience of critical infrastructure.

For citation

Grushitsyn A.S. (2025) Ekonomicheskiy aspekt ispol'zovaniya konechnykh poley Galua v zashchite informatsii [The Economic Aspect of Using Galois Finite Fields in Information Security]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (12A), pp. 611-617. DOI: 10.34670/AR.2026.42.70.050

Keywords

Information security, digital economy, Galois finite fields, cryptography, economic factor, quantum computing, post-quantum cryptography, cyber risks, security investments, technological sovereignty, critical infrastructure.

References

1. Bardis, N.G. et al. (2012). Fast implementation zero knowledge identification schemes using the Galois Fields arithmetic. In 2012 IX International Symposium on Telecommunications (BIHTEL) (pp. 1-6). IEEE. https://doi.org/[DOI not provided in source]
2. Chang, L.N. (2014). Quantum Systems based upon Galois Fields — from Sub-quantum to Super-quantum Correlations (Doctoral dissertation or Report). Virginia Tech.
3. Davletova, A. et al. (2024). Enhancing Cryptographic System Security based on Finite Fields. In 2024 14th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 476-480). IEEE. https://doi.org/[DOI not provided in source]
4. George, K., & Michaels, A.J. (2021). Designing a block cipher in Galois extension fields for IoT security. IoT, 2(4), 669-687. https://doi.org/[DOI not provided in source]
5. Hazzazi, M.M. et al. (2023). A novel cipher-based data encryption with galois field theory. Sensors, 23(6), 3287. https://doi.org/[DOI not provided in source]
6. Johnston, E.R. (2021). Programmirovanie kvantovykh komp'iuterov [Programming quantum computers] (Translated into Russian). St. Petersburg: Piter. (Original work published ?).
7. Nardo, L.G. et al. (2021). A reliable chaos-based cryptography using Galois field. Chaos: An Interdisciplinary Journal of Nonlinear Science, 31(9). [Pagination not provided in source]. https://doi.org/[DOI not provided in source]
8. Stupina, M.V. (2024). Razrabotka podkhoda k obespecheniiu informatsionnoi bezopasnosti v veb-orientirovannykh informatsionnykh sistemakh pri peredache dannykh s ispol'zovaniem interfeisa Web Cryptography API [Developing an approach to ensuring information security in web-oriented information systems for data transmission using the Web Cryptography API]. Izvestiia Kabardino-Balkarskogo nauchnogo tsentra RAN [Proceedings of the Kabardino-Balkarian Scientific Centre of the Russian Academy of Sciences], 26(1). [Pagination not provided in source].
9. Tarannikov, Iu.V. (2023). Samokorrektiruiushchiesia kody i ikh primeneniia v kriptografii [Self-correcting codes and their applications in cryptography]. Moscow: Moskovskii gosudarstvennyi universitet (MGU). [Примечание: Формат указывает на монографию или диссертацию. Если это статья в журнале, требуется уточнение названия издания, номера и страниц].
10. Zhang, Y. et al. (2024). The probabilistic image encryption algorithm based on galois field GF (257). IETE Journal of Research, 70(7), 6286-6299. https://doi.org/[DOI not provided in source]