МРНТИ 65.50.10 https://doi.org/10.48184/2304-568X-2025-4-5-14

ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УКРЕПЛЕНИЯ ПРОДОВОЛЬСТВЕННОЙ БЕЗОПАСНОСТИ: ТЕХНОЛОГИЧЕСКИЕ И ПРАВОВЫЕ ПОДХОДЫ

*[1]А.Б. ОМАРОВА , [1]Ш.Б. МАЛИКОВА , [2]Ж. С. САПАРБЕКОВА **

([1]Университет Нархоз, Казахстан, 050035, г. Алматы, ул. Жандосова 55
[2]Казахский национальный университет имени аль-Фараби, Республика Казахстан,
050040, г. Алматы, проспект Аль-Фараби, 71)
Электронная почта автора-корреспондента: Zhake9344@mail.ru*

Целью статьи является синтез современных технологических решений на базе больших данных и искусственного интеллекта для обеспечения пищевой безопасности и прослеживаемости, а также анализ правовых режимов, определяющих допустимость и требования к их применению в Казахстане, Евразийском экономическом союзе и Европейском союзе. Методологию составляет нарративный обзор нормативных актов, международных стандартов и научных публикаций с фокусом на интеграции цифровых технологий, управлении рисками, защите персональных данных, прозрачности алгоритмов. Уделено внимание системе управления безопасностью пищевых продуктов HACCP. Показано, что сочетание ISO 22000 и ISO 22005 с моделью событий GS1 EPCIS, датчиками IoT и алгоритмами машинного обучения обеспечивает ускоренную идентификацию опасностей, отзывы продукции и повышение достоверности доказательств при проверках. Предложена практическая дорожная карта «compliance-by-design»: определение единицы прослеживаемости. Сделан вывод о необходимости междисциплинарной интеграции технологических и правовых решений для устойчивого повышения безопасности продуктов питания. Научная статья подготовлена в рамках финансирования по научным и (или) научно-техническим программам на 2024-2026 годы, направленная на реализацию проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Ключевые слова: пищевое право; прослеживаемость; большие данные; искусственный интеллект; аутентичность; GDPR; ISO 22000; ISO 22005; GS1 EPCIS; NIS2.

АЗЫҚ-ТҮЛІК ҚАУІПСІЗДІГІН НЫҒАЙТУ ҮШІН ҮЛКЕН ДЕРЕКТЕР МЕН ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ: ТЕХНОЛОГИЯЛЫҚ ЖӘНЕ ҚҰҚЫҚТЫҚ ТӘСІЛДЕР

*[1]А.Б. ОМАРОВА, [1]Ш.Б. МАЛИКОВА, [2]Ж. С.САПАРБЕКОВА**

([1]Нархоз Университеті, Қазақстан, 050035, Алматы қ., Жандосов көшесі, 55
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан Республикасы,
050040, Алматы қ., әл – Фараби даңғылы, 71)
Автор-корреспонденттің электрондық поштасы:Zhake9344@mail.ru*

Мақалада үлкен деректер мен жасанды интеллект негізіндегі заманауи технологиялық шешімдердің тағам қауіпсіздігі мен өнімді қадағалаудағы рөлі қарастырылған. Қазақстан, Еуразиялық экономикалық одақ және Еуропалық одақ аясындағы құқықтық режимдер мен олардың қолдану талаптарына талдау жасалды. Зерттеу әдіснамасы - нормативтік актілер мен халықаралық стандарттарға, сондай-ақ ғылыми жарияланымдарға негізделген нарративтік шолу. HACCP жүйесіне цифрлық технологияларды енгізу, тәуекелдерді басқару, дербес деректерді қорғау, алгоритмдердің ашықтығы мен киберқауіпсіздік мәселелеріне ерекше назар аударылған. ISO 22000 және ISO 22005 стандарттарының GS1 EPCIS, IoT сенсорлары және машиналық оқыту алгоритмдерімен үйлесімі қауіпті факторларды жедел анықтауға және өнімді тиімді кері қайтарып алуға мүмкіндік беретіні көрсетілді. Авторлар «compliance by design» тәсілі негізінде құқықтық және технологиялық шешімдерді біріктірудің маңыздылығын көрсетті. Ғылыми мақала ИРН AP23489796 «Үлкен деректердің (Big Data) құқықтық режимін реттеу мәселелері: отандық және халықаралық тәжірибе» жобасы бойынша Қазақстан Республикасы Ғылым және жоғары білім министрлігінің ғылым комитеті қаржыландырған 2024-2026 жж. арналған ғылыми және ғылыми-техникалық бағдарламаларды қаржыландыру шеңберінде дайындалған.

Негізгі сөздер: азық-түлік қауіпсіздігі, үлкен деректер, жасанды интеллект, қадағалану, дербес деректер, стандарттау.

USING BIG DATA AND ARTIFICIAL INTELLIGENCE TO STRENGTHEN FOOD SECURITY: TECHNOLOGICAL AND LEGAL APPROACHES

[1]A.B. OMAROVA, [1]SH.B. MALIKOVA, [2]ZH. SAPARBEKOVA

([1]Narxoz University, Kazakhstan, 050035, Almaty, Zhandosov str., 55
[2]Al-Farabi Kazakh National University,Kazakhstan, 050040, Almaty, al-Farabi ave., 71)
Corresponding author's e-mail: zhake9344@mail.ru*

The paper reviews modern technological solutions based on big data and artificial intelligence for ensuring food safety and traceability, and analyzes the legal frameworks governing their application in Kazakhstan, the Eurasian Economic Union, and the European Union. The study employs a narrative review of regulatory acts, international standards, and academic publications focusing on the integration of digital technologies into HACCP systems, official control, risk management, data protection, algorithmic transparency, and cyber resilience. It is demonstrated that combining ISO 22000 and ISO 22005 with the GS1 EPCIS event model, IoT sensors, and machine learning algorithms enables faster hazard identification, targeted product recalls, and improved evidentiary reliability in audits, provided compliance with GDPR, the EU AI Act, NIS2, the Transparency Regulation, and national data protection laws. A "compliance by design" roadmap is proposed to integrate technological and legal solutions for sustainable food safety improvement. The scientific article was prepared within the framework of funding for scientific and (or) scientific and technical programs for 2024-2026, aimed at the implementation of the IRN project AP23489796 "Problems of regulating the legal regime of big data: domestic and international experience", funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan.

Keywords: big data, artificial intelligence, food safety, traceability, cyber resilience, GDPR, HACCP, EPCIS, NIS2, ISO 22000.

Введение

Настоящее исследование освещает технологические инновации и правовые аспекты, необходимые для ответственного внедрения цифровых технологий в пищевую промышленность. Пищевое право трактует прослеживаемость как инструмент адресной и соразмерной защиты здоровья населения и добросовестной торговли. Базовый Регламент ЕС № 178/2002 устанавливает обязанность знать «шаг назад – шаг вперёд» по каждой партии, а Регламент (ЕС) 2017/625 закрепляет полномочия официального контроля и ожидание наличия достоверных записей и воспроизводимых доказательств [1; 2]. Гигиеническое законодательство на основе международно признанной системы управления безопасностью пищевых продуктов «Анализ рисков и критические контрольные точки» (HACCP) связывает опасности, критические пределы, мониторинг, корректирующие действия и документирование, что в цифровую эпоху естественно опирается на датчики, события и метаданные [3]. В этой рамке большие данные и ИИ перестают быть экзотикой и превращаются в способ исполнения уже существующих обязанностей. Практическая значимость темы для Казахстана и ЕАЭС определяется действием ТР ТС 021/2011 «О безопасности пищевой продукции», переходом к электронным сертификатам и возрастающими требованиями к прослеживаемости, а также развитием национального регулирования персональных данных [4; 5].

Обеспечение пищевой безопасности остается критически важной мировой проблемой. По оценкам Всемирной организации здравоохранения, каждый десятый житель планеты ежегодно заболевает из-за употребления небезопасных продуктов питания [6]. Глобализация и усложнение цепочек поставок создали новые риски: продукты проходят длинный путь «от фермы до стола», что затрудняет контроль и своевременное выявление загрязнений. В этих условиях появляются инновационные подходы на основе больших данных и искусственного интеллекта (ИИ), призванные повысить оперативность и точность обеспечения безопасности пищевой продукции.

Современные цифровые технологии открывают широкие возможности для

мониторинга и прослеживаемости. ИИ вместе с сенсорами Интернета вещей (IoT) позволяет в реальном времени отслеживать критические параметры производства и логистики, выявлять отклонения и прогнозировать угрозы до того, как они приведут к массовым инцидентама gronews.comresearchgate.net.

К примеру, алгоритмы машинного обучения способны автоматически контролировать сроки годности и условия хранения, сигнализировать о нарушениях температурного режима и даже предсказывать появление контаминации.

Прослеживаемость продукции существенно усиливается за счет использования стандартов вроде ISO 22005 (международный стандарт по прослеживаемости кормов и пищевой продукции) и модели событий GS1 EPCIS, которые помогают документально фиксировать путь каждой партии товара.

Кроме того, аналитические методы на основе спектральных данных в сочетании с ИИ уже применяются для проверки аутентичности продуктов и обнаружения мошенничества (фальсификации состава), что повышает доверие к качеству продовольствия [7; 8]

Однако внедрение больших данных и ИИ в пищевую индустрию сталкивается с серьезными регуляторными и правовыми вызовами. Базовым требованием во всех юрисдикциях остается соблюдение принципов системы HACCP (анализ опасностей и критические контрольные точки) – фундаментальной методологии управления рисками пищевой безопасности. Например, в Европейском союзе все предприятия пищевой отрасли (за исключением первичных производителей) обязаны внедрить процедуры на основе HACCPeur-lex.europa.eu, аналогичные требования закреплены и в технических регламентах Евразийского экономического союза, в частности ТР ТС 021/2011 «О безопасности пищевой продукции» [9].

Таким образом, цифровые инновации должны интегрироваться в существующие системы менеджмента безопасности пищевых продуктов (например, стандарты ISO 22000 [10], основанные на принципах HACCP) без нарушения их целостности.

Помимо технологической реализации, остро встают вопросы правового соответствия и этики использования данных. В регионе ЕС действуют строгие нормы защиты персональных данных – General Data Protection Regulation (GDPR) [11], устанавливающие ограничения на сбор и обработку информации о потребителях. Планируемый Акт ЕС об искусственном интеллекте предъявляет требования прозрачности и управляемости алгоритмов, особенно при использовании ИИ в сферах высокого риска, к которым может относиться пищевая промышленность. Директива NIS2 усиливает требования к кибербезопасности критически важных систем, включающих продовольственные цепочки.

В Казахстане и странах ЕАЭС эти тенденции отражаются в адаптации национального законодательства. В Казахстане действует собственный закон о персональных данных, а механизмы государственного официального контроля опираются на нормативы ЕАЭС (включая упомянутый ТР ТС 021/2011).

Однако, пока отсутствуют детально проработанные правила по обращению с алгоритмами ИИ и большими данными в контексте пищевой безопасности, что создает правовые пробелы. Необходимо обеспечить баланс между инновациями и соблюдением требований по конфиденциальности, прозрачности и ответственности.

Как отмечают исследователи, для широкого внедрения цифровых технологий в пищевой сектор предстоит решить проблемы стандартизации данных и защиты приватности [13].

Настоящий обзор нацелен на междисциплинарный анализ указанных вопросов. В нем обобщаются современные технологические решения, основанные на больших данных и ИИ, для повышения безопасности пищевых продуктов и просле-живаемости - от ускоренного выявления опасностей до точечного отзыва продукции и обнаружения фальсификаций. Одновременно рассматриваются правовые режимы, определяющие допустимость применения этих технологий, и требования регуляторов в Казахстане, Евразийском экономическом союзе и Европейском союзе. Таким образом, формируется целостная картина того, как технологические инновации могут интегрироваться с принципом «compliance by design» (встроенного соблюдения регуляторных требований с этапа проектирования систем) для устойчивого повышения уровня пищевой безопасности в глобальном и региональном контексте.

Материалы и методы исследований

Методологию составляет нарративный обзор нормативных актов, международных стандартов и научных публикаций с фокусом на интеграции цифровых технологий в системы HACCP [15], официальном контроле, управлении

рисками, защите персональных данных, прозрачности алгоритмов и киберустойчивости. Проведен анализ нормативных актов ЕС, ЕАЭС и Республики Казахстан, международных стандартов и профильной научной литературы в частях прослеживаемости, HACCP, защиты данных, алгоритмической прозрачности и киберустойчивости. Указанные материалы задействованы как методические источники.

Современные системы обеспечения пищевой безопасности переживают этап глубокой цифровой трансформации, обусловленной ростом объёмов данных, усложнением цепей поставок и усилением требований к прозрачности и контролю происхождения продукции. В условиях глобализации продовольственных рынков традиционные методы инспекций и документального учёта уже не обеспечивают необходимой скорости и точности при выявлении рисков загрязнения, фальсификации и несоответствия стандартам качества. На первый план выходят технологии обработки больших данных и искусственного интеллекта, способные интегрировать разнородные источники информации, анализировать динамические потоки данных и прогнозировать угрозы в реальном времени.

Развитие таких подходов изменяет парадигму управления безопасностью продуктов питания, смещая акцент с реактивного контроля на превентивную аналитику и интеллектуальную автоматизацию процессов. Использование алгоритмов машинного обучения и датчиков интернета вещей позволяет не только повысить точность обнаружения отклонений и аномалий, но и создать непрерывно обновляемую цифровую модель прослеживаемости продукции на всех этапах её жизненного цикла. Это усиливает доверие потребителей и регулирующих органов к доказательной базе контроля, а также снижает вероятность человеческих ошибок и затраты на проверки и изъятия продукции.

Однако широкое внедрение технологий искусственного интеллекта и больших данных в агропродовольственном секторе сопровождается сложными правовыми и этическими вопросами. Возникает необходимость согласования таких решений с нормами о защите персональных данных, прозрачности алгоритмов, киберустойчивости и распределении ответственности между участниками цепи поставок. В Европейском союзе эти вопросы регулируются рядом актов, включая Общий регламент по защите данных, Акт об искусственном интеллекте и директиву NIS2. В государствах Евразийского экономического союза и Казахстане формируется собственная норма-тивная база, стремящаяся к гармонизации с международными стандартами ISO 22000 и ISO 22005, а также с требованиями технических регламентов и национального законодательства о цифровой безопасности.

Таким образом, исследование сосредоточено на анализе взаимосвязи между технологическими инновациями и правовыми режимами, определяющими возможности внедрения решений на базе больших данных и искусственного интеллекта в сфере пищевой безопасности. Целью является выявление оптимальных моделей интеграции цифровых технологий в систему управления рисками, официального контроля и прослеживаемости, а также разработка подходов к обеспечению правомерности и устойчивости таких систем в разных правовых юрисдикциях.

Результаты и их обсуждение

Одним из обсуждаемых тем стали технологические инновации в области пищевой безопасности, поскольку продвижение аналитики больших данных, устройств Интернета вещей (IoT) и искусственного интеллекта (ИИ) приводит к трансформационным улучшениям в управлении безопасностью пищевой продукции. Большие данные и IoT обеспечивают сквозную прослеживаемость цепочек поставок «от фермы до стола» с беспрецедентной прозрачностью [16]. Например, датчики IoT (температуры, влажности и др.), установленные на пищевых грузах, непрерывно фиксируют условия транспортировки, а данные доступны в реальном времени.

Ключевую роль в этом процессе играет внедрение глобальных стандартов, таких как GS1 EPCIS (Electronic Product Code Information Services - сервисы обмена информацией по электронному коду продукции), для обмена событийными данными: версия EPCIS 2.0 позволяет включать показания сенсоров (температура, влажность и т.п.) по мере движения продукции по цепочке. Это означает, что при отклонении условий хранения от нормативных значений партия может быть мгновенно идентифицирована и изолирована, предотвращая потенциальный инцидент в сфере безопасности [17]. В совокупности это дает новый уровень видимости цепи поставок и оперативности реагирования на опасности и проблемы качества.

Параллельно методы ИИ усиливают безопасность за счет улучшенного обнаружения и прогнозной аналитики. Модели машинного обучения анализируют потоки производственных и логистических данных, выявляя

закономерности, связанные с риском контаминации. Так, алгоритмы с учителем обучаются на исторических технологических данных (температура, pH, микробная обсемененность и др.) и в реальном времени помечают аномалии, напоминающие условия, предшествовавшие прежним инцидентам. Системы компьютерного зрения на базе сверточных нейронных сетей (CNN) распознают мельчайшие дефекты или посторонние включения на конвейере, предотвращая попадание некондиционной или опасной продукции к потребителю [18].

Кроме того, подходы сенсорного слияния - «электронный нос» и «электронный язык», интегрированные с моделями ИИ, - выявляют порчу или фальсификацию по химическим сигнатурам (например, газы порчи в мясе или добавки в молоке). Эти умные методы детекции позволяют раньше и надежнее идентифицировать опасности, поддерживая превентивную парадигму (в соответствии с принципами HACCP). Прогнозная аналитика на базе ИИ также улучшает управление рисками в цепи поставок - от более точного прогноза сроков годности и порчи до оценки влияния погодных событий на логистику [19].

Важна и эффективность с доверием потребителей. Сквозная цифровая прослеживаемость повышает способность компаний быстро и точно проводить отзывы: каждый ингредиент и продукт отслеживаемы до источника и маршрута распределения. Технологии блокчейна усиливают доверие, формируя неизменяемые записи на каждом этапе. Блокчейн-системы присваивают каждому продукту уникальный цифровой идентификатор и фиксируют его «жизненный путь» (происхождение сырья, операции переработки, номера партий) в распределенном реестре, что повышает уверенность потребителей в безопасности и подлинности. В итоге оцифровка управления безопасностью - через платформы больших данных, IoT-сенсорику и аналитику ИИ - дает значимые результаты: ускоренное выявление опасностей, большая прозрачность, более эффективное соблюдение стандартов и лучшая гарантия качества от производства до потребления [18]. Внедрение больших данных и ИИ в пищевую отрасль происходит в условиях жестких регуляторных рамок. Ключевые аспекты - защита персональных данных, их конфиденциальность и кибербезопасность. В части конфиденциальности Общий регламент по защите данных ЕС (GDPR) предъявляет строгие требования к любой обработке персональных данных, что затрагивает цепочки поставок и системы безопасности. Пищевые компании часто обрабатывают персональные данные потребителей, поставщиков и сотрудников. Если речь идет о резидентах ЕС, GDPR применяется вне зависимости от местоположения оператора. Требуются законные основания обработки (согласие, легитимный интерес и др.), а также меры минимизации и псевдонимизации. Важна и ст. 22 GDPR, ограничивающая полностью автоматизированные решения с существенным воздействием. Например, если ИИ автоматически отклоняет сырье или прекращает работу с поставщиком на основе риск-скоринга, необходимы прозрачность и участие человека. За несоблюдение предусмотрены штрафы до 20 млн евро или 4% глобального оборота (что больше) [19]. Следовательно, инновации на базе больших данных должны внедряться с учетом «privacy-by-design» и процедур контроля соответствия.

Правила кибербезопасности в ЕС системно охватывает Директива NIS2 (Directive (EU) 2022/2555). Продовольственные цепочки включены в перечень критических секторов. Поэтому средние и крупные компании пищевой отрасли рассматриваются как «существенные» или «важные» субъекты и обязаны выполнять требования по управлению киберрисками [12].

NIS2 требует «соразмерных технических и организационных мер»: регулярные оценивания рисков, планы реагирования на инциденты, обеспечение непрерывности (резервное копирование, восстановление), безопасность цепочек поставок, базовая гигиена (контроль доступа, шифрование, обучение персонала). Поскольку современные системы безопасности опираются на IoT-устройства и облака, поверхность атаки значительна: компрометация целостности данных сенсоров или отказ платформ прослеживаемости напрямую влияет на безопасность. NIS2 вводит и обязанности уведомления: значимые инциденты нужно сообщать регуляторам в сжатые сроки (предварительно в течение 24 часов, затем подробности к 72-й час). Для «важных» субъектов предусмотрены штрафы [12]. Иными словами, киберустойчивость становится опорой пищевой безопасности.

За пределами ЕС действуют сопоставимые подходы. В государствах ЕАЭС (в т.ч. Казахстан) применяются технические регламенты, регулирующие безопасность и прослеживаемость пищевой продукции. Международные стандарты Codex Alimentarius [21] поощряют прослеживаемость и прозрачность. Дискуссии вокруг

Акта ЕС об ИИ добавляют требования к прозрачности и контролю алгоритмов при применении ИИ в сферах повышенного риска. В Казахстане действует собственный закон о персональных данных, а механизмы официального контроля опираются на нормы ЕАЭС.

Для понимания среды регулирования были сопоставлены три рамки, релевантные большим данным и ИИ в пищевой безопасности - GDPR (персональные данные), директива NIS2 (кибербезопасность) и Технический регламент Таможенного союза ТР ТС 021/2011 «О безопасности пищевой продукции». Результаты сравнения представлены в Таблице 1, где показаны положения каждой из них и их связь с технологическими инновациями.

Таблица 1. Сопоставление ключевых регуляторных рамок: GDP, директивы NIS2, Технический регламент Таможенного союза ТР ТС 021/2011

Регламент	**Сфера и отрасль**	**Ключевые требования к данным/технологиям**	**Надзор и санкции**
GDPR (ЕС, 2018)	Любая организация, обрабатывающая персональные данные резидентов ЕС (включая производителей, ритейл и поставщиков, работающих с данными покупателей/сотрудников) [1]. Горизонтальный закон о данных.	- Законность и прозрачность обработки (согласие/иное основание); - Защита данных по замыслу: приватность в архитектуре аналитических и IoT-систем (шифрование, минимизация); - Права субъектов (доступ, удаление, исправление) в контексте больших данных; - Ограничения на полностью автоматизированные решения с существенным эффектом (актуально для автономных решений ИИ).	Штрафы до 20 млн евро или 4% мирового оборота. Надзор – национальные органы по защите данных, с трансграничной координацией.
NIS2 (ЕС, 2024)	Средние и крупные компании пищевого сектора как часть критической инфраструктуры [2].	- Управление киберрисками: меры тех/орг/операционного уровня (оценки рисков, реагирование на инциденты, непрерывность, безопасность цепочек поставок, контроль доступа и др.); - Уведомление об инцидентах в установленные сроки [2]; - Контроль поставщиков (аудит облаков/ПО/IoT), т.к. уязвимости третьих сторон могут затронуть операции [2]; - Постоянный надзор и доказательная база соответствия.	Транспозиция до окт. 2024; штрафы до 1,4% оборота или 7 млн евро (для «важных» субъектов); возможны предписания, приостановка сертификатов.
ТР ТС 021/2011 (ЕАЭС, 2013)	Пищевая продукция и субъекты оборота в ЕАЭС (Россия, Казахстан, Беларусь и др.). Регламент безопасности пищевой продукции.	- Требования к безопасности продукта (ограничения контаминантов, гигиена, системы управления безопасностью по аналогии с HACCP); - Прослеживаемость: сопровождающие документы (бумажные или электронные) с идентификацией производителя и последующих владельцев; - Маркировка и информирование (состав, сроки годности, происхождение и др.); - Оценка соответствия (сертификация/декларирование) до вывода на рынок. При этом глубина прослеживаемости ниже, чем в ЕС: акцент на принципе «один шаг назад - один шаг вперед».	Обязательная оценка соответствия; маркировка знаком ЕАС. При несоответствии отказ в сертификации/запрет оборота, национальные санкции (штрафы, отзыв).

Как видно из Таблицы 1, GDPR фокусируется на персональных данных, NIS2 – на кибербезопасности критических систем (включая используемые в продовольственных цепочках), а ТР ТС 021/2011 – на собственно безопасности и прослеживаемости пищевой продукции. Совместно они формируют «ограждения», в рамках которых цифровые инновации должны реализовываться этично, безопасно и с соблюдением качества.

В целом анализ демонстрирует тенденцию к усилению надзора на стыке технологий

и пищевой безопасности. Законы о данных (GDPR и аналоги) обеспечивают этичность и прозрачность аналитики больших массивов; мандаты по кибербезопасности (NIS2 и др.) адресуют новые уязвимости цифровой трансформации; профильные нормы (ТР ТС 021/2011 и регламенты ЕС) продолжают требовать прослеживаемости и контроля безопасности, развиваясь в такт с технологиями.

Показателен пример США (FSMA), где Правило 204 вводит электронную прослеживаемость для ряда «высокорисковых» продуктов [22], что подчеркивает растущую роль цифровых записей и оперативного доступа к данным. Технологии и регулирование движутся синхронно: большие данные и ИИ дают инструменты повышения безопасности, а регуляторы - рамки для их ответственного применения.

Также показательным может использование IoT, ИИ и данных, например, для прослеживаемости молочной продукции. Молочная цепочка поставок – прослеживаемость партии молока от фермы до розницы. Молочная продукция скоропортящаяся и чувствительна к температурному режиму. Молоко – традиционная мишень фальсификации (разбавление, добавки). Современные решения IoT и данных успешно применяются в этой сфере [23]. Сочетание GS1 EPCIS и IoT-сенсоров обеспечивает отслеживание партии в реальном времени. Каждой партии сырого молока присваивается уникальный идентификатор (QR/RFID на автоцистерне/контейнере). По мере продвижения – от фермерского танка-охладителя, к сборщику, на молочный завод, далее к дистрибьюторам и магазинам – фиксируются ключевые события отслеживания (CTE) в EPCIS-совместимой базе, то есть фиксируется время дойки и локация фермы, отбор автоцистерной (с отметкой времени и GPS), параметры пастеризации (номер линии/партии, температура), фасовка с кодами партий, отгрузка и приемка [9]. Датчики температуры в автоцистернах и силосах ведут непрерывный лог. При выходе параметров за допустимые пределы система формирует тревогу. Если, например, смарт-контракт на блокчейне связан с IoT-данными и, если поставка соблюдала температурный режим и пришла вовремя, смарт-контракт может автоматически инициировать оплату за поставленную продукцию. В противном случае - приостановить платеж и запустить расследование [7]. Преимущества для потребителей и регуляторов очевидны. Потребитель, отсканировав код на упаковке, через платформы вроде fTRACE получает сведения об источнике партии, времени и месте переработки, характеристиках фермы [24]. Такой уровень прозрачности укрепляет доверие к бренду и помогает делать осознанный выбор.

Для регуляторов полная прослеживаемость обеспечивает выполнение требований ТР ТС 021/2011 о документальном сопровождении и идентификации и правил ЕС (ст. 18 Регламента (ЕС) № 178/2002) по принципу «один шаг назад – один шаг вперед». В случае инцидента (например, выявление порчи йогурта) производитель, считав код, извлекает историю производства: партия сырого молока, ферма-источник, иные ингредиенты, данные линии, дистрибуция - и в считанные часы проводит точечный отзыв и устраняет причину (скажем, сбой температуры в конкретной автоцистерне в жаркий день).

Указанный пример демонстрирует практические результаты интеграции больших данных и ИИ, то есть стандартизованный обмен данными (EPCIS), IoT-мониторинг и автоматизация на базе ИИ, блокчейна образуют мощный инструментарий обеспечения безопасности и комплаенса. Он отвечает запросам потребителей на прозрачность и требованиям регуляторов к прослеживаемости и подотчетности.

Вместе с тем реализация требует инвестиций в цифровую инфраструктуру и обучение. Для малых производителей это может быть барьером. Критична интероперабельность данных, то есть опыт инициатив вроде Global Dialogue on Seafood Traceability показывает ценность общих стандартов в трансграничных цепочках [25], аналогичные подходы укрепляются и в молочной отрасли. По мере удешевления и зрелости технологий такие решения станут отраслевым стандартом, снижая вероятность крупномасштабных инцидентов пищевой безопасности.

Заключение

Результаты анализа показывают, что использование больших данных и ИИ (через улучшение прослеживаемости, прогнозную аналитику и ускоренное реагирование) существенно снижает риски, а при поддержке адекватных регуляторных рамок и отраслевого взаимодействия прокладывает путь к более безопасному и прозрачному продовольствен-

ному снабжению - от производителя пищевой продукции и так далее.

Цифровая прослеживаемость и аналитика на базе больших данных и ИИ усиливают действенность пищевого права, поскольку делают возможными раннюю идентификацию опасностей, точечные отзывы и доказательно выверенные решения. Технологический эффект реализуется только при соблюдении правовых требований к защите данных, прозрачности алгоритмов и киберустойчивости, а также при наличии договорных механизмов переноси-мости и аудита. Наиболее рациональной стратегией для предприятий становится «compliance-by-design»: начать с единицы прослеживаемости и стандарта событий, параллельно выстроить правовые основания и DPIA, внедрить мониторинг моделей и обеспечить готовность аудиторских пакетов. Междисциплинарная кооперация специалистов по качеству, юристов, ИТ-инженеров и учёных-данных является ключевым фактором устойчивого повышения безопасности пище-вой продукции в Казахстане, ЕАЭС и ЕС.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Регламент (ЕС) 2017/625 Европейского Парламента и Совета от 15 марта 2017 «Об официальном контроле и других официальных мероприятиях, проводимых с целью обеспечения применения пищевого и кормового законодательства, санитарных норм и правил о благополучии животных, здоровье растений и средствах защиты растений». –- [Электронный ресурс]. – 2025- URL: https://fsvps.gov.ru/files/reglament-es-2017-625-evropejskogo-parlamen/.

2. D. Sedik «Food Safety Control in the EU and EAEU», University of Halle, 2016.

3. Barcoding.com Blog, «How Data Capture Tech is Modernizing the Food Supply Chain», 2022.

4. Технический регламент Таможенного союза ТР ТС 021/2011 «О безопасности пищевой продукции». Москва: ЕЭК, 2011 - [Электронный ресурс]. – 2025- URL: http://www.eurasian-commission.org (дата обращения: 14.06.2025).

5. Закон Республики Казахстан «О персональных данных и их защите» от 21.05.2013 № 94-V. [Электрондық ресурс]. – 2025- URL: https://adilet.zan.kz (дата обращения: 14.06.2025).

6. Искусственный интеллект меняет подход к производству мороженого в Казахстане. – [Электронный ресурс]. – 2025- URL: https://agronews.com/kz/ru/news/breaking-news/2025-0528/59225#:~:text=%D0%A1%D0%BE%D0%B3%D0%BB%D0%B0%D1%81%D0%BD%D0%BE%20%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%BC%20%D0%92%D1%81%D0%B5%D0%BC%D0%B8%D1%80%D0%BD%D0%BE%D0%B9%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B7%D0%B4%D1%80%D0%B0%D0%B2%D0%BE%D0%BE%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F%2C,%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%B8%D1%82%D0%B5%D0%BB%D0%B5%D0%B9%2C%20%D1%82%D0%B0%D0%BA%20%D0%B8%20%D1%81%D0%B0%D0%BC%D0%B8%D1%85%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B9

7. Искусственный интеллект, большие данные и блокчейн в безопасности пищевых продуктов – [Электронный ресурс]. – 2025- URL: https://www.researchgate.net/publication/356357841_Artificial_intelligence_big_data_and_blockchain_in_food_safety

8. Выявление фальсификации пищевых продуктов с помощью анализа данных на основе искусственного интеллекта –[Электронный ресурс]. – 2025-URL: https://www.labmanager.com/detecting-food-fraud-through-ai-powered-data-analysis-30680

9. Технический регламент Таможенного союза ТР ТС 021/2011 «О безопасности пищевой продукции» (ЕАЭС) – [Электронный ресурс]. – 2025-URL: https://eec.eaeunion.org/comission/department/deptexreg/tr/PischevayaProd.php

10. Data Protection Regulation (GDPR) – [Электронный ресурс]. – 2025- URL: https://gdpr-info.eu/

11. ISO 22000:2018. Food safety management systems - Requirements for any organization in the food chain. Geneva: ISO, 2018. –[Электронный ресурс]. – 2025- URL: https://www.bsigroup.com/globalassets/localfiles/en-ae/iso22000/guide-to-iso-22000/

12. Соответствие требованиям директивы кибербезопасности EU NIS 2 –[Электронный ресурс]. – 2025- URL: https://www.h-x.technology/ru/services/nis-2-cybersecurity-directive-ru

13. Храмов Александр Алексеевич. Инновационные технологии в эпоху цифровой трансформации: анализ и перспективы // Journal of Monetary Economics and Management. 2024. №8. [Электронный ресурс]. – 2025- URL: https://cyber-leninka.ru/article/n/innovatsionnye-tehnologii-v-epohu-tsifrovoy-transformatsii-analiz-i-perspektivy (дата обращения: 14.10.2025).

14. Thomas Fox. Compliance by Design: Future-Proofing Your Product Oversight and Governance – [Электронный ресурс]. – 2025- URL: https://www. linkedin.com/pulse/compliance-design-future-proofing-your-product-oversight-thomas-fox-onjtc

15. СТ РК ISO 22000-2019 и HACCP – [Электронный ресурс]. – 2025- URL: http://abc-cert.kz/haccp .

16. Интернет вещей и новые решения для современных цепочек поставок: адаптация к изменениям рынка – [Электронный ресурс]. – 2025- URL: https://apni.ru/article/2045-internet-veshhej-i-novye-resheniya-dlya-sovremennyh-czepochek-postavok-adaptacziya-k-izmeneniyam-rynka

17. GS1 2025: Прокладывая мосты в будущее глобальных стандартов – [Электронный ресурс]. – 2025- URL: https://standard.kz/ru/post/2025_05_gs1-2025-prokladyvaia-mosty-v-budushhee-globalnyx-standartov-301

18. Gálvez J. F., Mejuto J. C., Simal-Gándara J. Future challenges on the use of blockchain for food traceability analysis // Trends in Analytical Chemistry. 2018. Vol. 107. P. 222–232. DOI: 10.1016/ j.trac.2018.08.001.

19. Электронный нос: перспективный многофункциональный прибор – [Электронный ресурс]. – 2025- URL: https://habr.com/ru/companies /first/articles/695986/

20. Are You Ready for GDPR? – [Электронный ресурс]. – 2025- URL: https://www.gartner.com/ smarterwithgartner/ready-guide-to-gdpr

21. Codex Alimentarius –[Электронный ресурс]. – 2025- URL: https://www.fao.org/food-safety/food-control-systems/policy-and-legal-frameworks/codex-alimentarius/ru/

22. FSMA 204 и безопасность пищевых продуктов: проверка требований соответствия [Электронный ресурс]. – 2025- URL: https://rfxcel. com/ru/fsma-204-data-carrier/

23. Пять примеров успешного использования ИИ на производстве - [Электронный ресурс]. – 2025- URL: https://habr.com/ru/articles/727358/

24. Повышайте лояльность клиентов с помощью интеллектуальной упаковки – [Электронный ресурс]. – 2025- URL: https://remos.ru/blog/a-blog-about packaging/marketing/ povyshayte-loyalnost-klientov-s-pomoshchyu-intellektualnoy-upakovki/

25. Компании по отслеживанию морепродуктов объединяются, чтобы упростить обмен данными и улучшить стандарты прослеживаемости морепродуктов – [Электронный ресурс]. – 2025- URL: https://www.global-seafood.org/advocate/topic/gdst/

REFERENCES

1. Reglament (ES) 2017/625 Evropejskogo Parlamenta i Soveta ot 15 marta 2017 «Ob oficialnom kontrole i drugih oficialnyh meropriyatiyah, provodimyh s celyu obespecheniya primeneniya pishevogo i kormovogo zakonodatelstva, sanitarnyh norm i pravil o blagopoluchii zhivotnyh, zdorove rastenij i sredstvah zashity rastenij». [On official control and other official activities carried out to ensure the enforcement of food and feed legislation, sanitary norms and rules on animal welfare, plant health, and plant protection products] – [Elektronnyi resurs]. – 2025. - URL: https://fsvps.gov.ru/files/reglament-es-2017-625-evropejskogo-parlamen/.

2. D. Sedik «Food Safety Control in the EU and EAEU», University of Halle, 2016.

3. Barcoding.com Blog, «How Data Capture Tech is Modernizing the Food Supply Chain», 2022.

4. Tehnicheskij reglament Tamozhennogo soyuza TR TS 021/2011 «O bezopasnosti pishevoj produkcii». Moskva: EEK, 2011. - . [Technical Regulation of the Customs Union TR CU 021/2011 «On the Safety of Food Products».] - [Elektronnyi resurs]. – 2025. - URL: http://www.eurasiancommission.org (data obrasheniya: 14.06.2025).

5. Zakon Respubliki Kazahstan «O personalnyh dannyh i ih zashite» ot 21.05.2013 № 94 V. - [Law of the Republic of Kazakhstan "On Personal Data and Its Protection" dated 21.05.2013 No. 94-V.] - [Elektronnyi resurs]. – 2025. - URL: https://adilet.zan.kz (data obrasheniya: 14.06.2025).

6. Iskusstvennyj intellekt menyaet podhod k proizvodstvu morozhenogo v Kazahstane. [Artificial intelligence is changing the approach to ice cream production in Kazakhstan.]– [Elektronnyi resurs]. – 2025. URL:https://agronews.com/kz/ru/news/breaking-news/2025-05-28/59225#:~:text= %D0%A1%D0% BE %D0%B3%D0%BB%D0%B0%D1%81%D0%BD%D0%BE%20%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%BC%20%D0%92%D1%81%D0%B5%D0%BC%D0%B8%D1%80%D0%BD%D0%BE%D0%B9%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B7%D0%B4%D1%80%D0%B0%D0%B2%D0%BE%D0%BE%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F%2C,%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%B8%D1%82%D0%B5%D0%BB%D0%B5%D0%B9%2C%20%D1%82%D0%B0%D0%BA%20%D0%B8%20%D1%81%D0%B0%D0%BC%D0%B8%D1%85%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B9

7. Iskusstvennyj intellekt, bolshie dannye i blokchejn v bezopasnosti pishevyh produktov – [Artificial Intelligence, Big Data, and Blockchain in Food Safety] - [Elektronnyi resurs]. – 2025.-URL: https://www.researchgate.net/publication/356357841_ Artificial_intelligence_big_data_and_blockchain_in_food_safety

8. Vyyavlenie falsifikacii pishevyh produktov s pomoshyu analiza dannyh na osnove iskusstvennogo intellekta - [Detection of food fraud using data analysis based on artificial intelligence] – [Elektronnyi resurs]. – 2025. - URL: https://www.labmanager .com/detecting -food-fraud-through-ai-powered-data-analysis-30680

9. Tehnicheskij reglament Tamozhennogo soyuza TR TS 021/2011 «O bezopasnosti pishevoj produkcii» - [Technical Regulation of the Customs Union TR CU 021/2011 'On the Safety of Food Products] (EAES) – [Elektronnyi resurs]. – 2025. -

URL: https://eec.eaeunion.org/comission/department /deptexreg/tr/PischevayaProd.php

10. General Data Protection Regulation (GDPR) – [Elektronnyi resurs]. – 2025. - URL: https://gdpr-info.eu/

11. ISO 22000:2018. Food safety management systems - Requirements for any organization in the food chain. Geneva: ISO, 2018. – [Elektronnyi resurs]. – 2025. - URL: https://www.bsigroup.com/globalassets/ localfiles/en-ae/iso22000/guide-to-iso-22000/

12. Sootvetstvie trebovaniyam direktivy kiberbezopasnosti EU NIS 2 - [Compliance with the requirements of the Cybersecurity Directive] – [Elektronnyi resurs]. – 2025. - URL: https://www.h-x.technology/ru/services/nis-2-cybersecurity-directive-ru

13. Hramov Aleksandr Alekseevich Innovacionnye tehnologii v epohu cifrovoj transformacii: analiz i perspektivy - [Innovative Technologies in the Era of Digital Transformation: Analysis and Prospects] // Journal of Monetary Economics and Management. 2024. №8. [Elektronnyi resurs]. – 2025. - URL: https://cyberleninka. ru/article/n/innovatsionnye-tehnologii-v-epohu-tsifrovoy-transformatsii-analiz-i-perspektivy (data obrasheniya: 14.10.2025).

14. Thomas Fox. Compliance by Design: Future-Proofing Your Product Oversight and Governance– [Elektronnyi resurs]. – 2025. - URL: https://www. linkedin. com/pulse/compliance-design-future-proofing -your-product-oversight-thomas-fox-onjtc

15. ST RK ISO 22000-2019 i HACCP [Elektronnyi resurs]. – 2025. - URL: http://abc-cert.kz/haccp.

16. Internet veshej i novye resheniya dlya sovremennyh cepochek postavok: adaptaciya k izmeneniyam rynka - [The Internet of Things and New Solutions for Modern Supply Chains: Adapting to Market Changes] – [Elektronnyi resurs]. – 2025. - URL: https://apni.ru/article/2045-internet-veshhej-i-novye-resheniya-dlya-sovremennyh-czepochek-postavok-adaptacziya-k-izmeneniyam-rynka

17. GS1 2025: Prokladyvaya mosty v budushee globalnyh standartov - [Building bridges to the future of global standards] – [Elektronnyi resurs]. – 2025. - URL:https://standard.kz/ru/post/2025_05_gs1-2025-prokladyvaia-mosty-v-budushhee-globalnyx-standartov-301

18. Galvez J. F., Mejuto J. C., Simal Gandara J. Future challenges on the use of blockchain for food traceability analysis // Trends in Analytical Chemistry. 2018. Vol. 107. P. 222–232. DOI: 10.1016 /j.trac.2018.08.001.

19. Elektronnyj nos: perspektivnyj mnogofunkcionalnyj pribor - [Electronic Nose: A Promising Multifunctional Device] – [Elektronnyi resurs]. – 2025. - URL: https://habr.com/ru/ companies/first/articles/695986/

20. Are You Ready for GDPR? – [Elektronnyi resurs] – 2025. - URL: https://www.gartner.com/ smarterwithgartner/ready-guide-to-gdpr

21. Codex Alimentarius – [Elektronnyi resurs]. – 2025. - URL: https://www.fao.org/food-safety/food-control-systems/policy-and-legal-frameworks/codex-alimentarius/ru/

22. FSMA 204 i bezopasnost pishevyh produktov: proverka trebovanij sootvetstviya - [FSMA 204 and food safety: compliance requirements verification] - [Elektronnyi resurs]. – 2025. - URL: https://rfxcel.com/ru/fsma-204-data-carrier/

23. Pyat primerov uspeshnogo ispolzovaniya II na proizvodstve - [Five examples of successful AI use in manufacturing] - [Elektronnyi resurs]. – 2025. - URL: https://habr.com/ru/articles/727358/

24. Povyshajte loyalnost klientov s pomoshyu intellektualnoj upakovki - [Increase customer loyalty with intelligent packaging] - [Elektronnyi resurs]. – 2025. - URL: https://remos.ru/blog/a-blog-about-packaging/marketing/povyshayte-loyalnost-klientov-s-pomoshchyu-intellektualnoy-upakovki/

25. Kompanii po otslezhivaniyu moreproduktov obedinyayutsya, chtoby uprostit obmen dannymi i uluchshit standarty proslezhivaemosti moreproduktov - [Seafood tracking companies are joining forces to streamline data sharing and improve seafood traceability standards] [Elektronnyi resurs] – 2025. - URL: https://www.globalseafood.org/advocate/topic/gdst/