Научная статья
УДК 338.436
doi: 10.55186/25876740_2026_69_3_417

КИБЕРБЕЗОПАСНОСТЬ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ РОССИИ: ИНСТРУМЕНТЫ, КЕЙСЫ, ИНЦИДЕНТЫ

Д.М. Назаров[1], Ю.В. Гудошникова[1], Н.В. Сербина[1], Н.Г. Протас[2]

[1]Уральский государственный экономический университет, Екатеринбург, Россия
[2]Новосибирский государственный университет экономики и управления, Новосибирск, Россия

Аннотация. Актуальность исследования определяется ускоренной цифровизацией агропромышленного комплекса России, ростом зависимости отрасли от информации, автоматизированных систем управления и государственных цифровых платформ прослеживаемости. Киберинциденты в аграрном секторе перестали быть сугубо ИТ-проблемой и затрагивают физическое производство, логистику, холодильные мощности и экспортные каналы. Публично описанные атаки на крупные российские агрохолдинги, логистические хабы, перерабатывающие предприятия и государственные информационные системы подтверждают переход угроз из плоскости конфиденциальности данных в плоскость операционной устойчивости и продовольственной безопасности. Цель исследования — систематизировать ландшафт киберугроз для агропромышленного комплекса России, описать доминирующие сценарии атак и проанализировать применяемые инструменты кибербезопасности и стандарты управления рисками с точки зрения их соответствия отраслевой специфике. Методически работа основана на качественном анализе научных публикаций по кибербезопасности сельского хозяйства и цифровому сельскому хозяйству, международных отраслевых отчётов по киберугрозам продовольственным и аграрным цепочкам, российских медийных и отраслевых кейсов кибератак, а также официальных нормативных документов, регулирующих защиту критической информационной инфраструктуры и информационных систем органов власти. Научная новизна заключается в комплексной увязке трёх уровней анализа: глобальной статистики атак на продовольственный и аграрный сектор, публично известных российских инцидентов в АПК и практик внедрения отраслевых решений по кибербезопасности. Предложена структурированная матрица, связывающая типы киберинцидентов в аграрных цепочках «поле — переработка — логистика — контроль и прослеживаемость» с кластерами инструментов (SOC/SIEM, EDR/XDR, защита OT/IoT, IRP/SOAR, DLP/DCAP) и рамочными стандартами управления рисками (ISO/IEC 27001, NIST CSF 2.0, российские требования к субъектам КИИ). В результате формируется отраслевой «минимальный стандарт» киберустойчивости, учитывающий специфику российских аграрных компаний и цифровых платформ государственного контроля.

Ключевые слова: киберинциденты, критическая информационная инфраструктура, управление киберрисками, продовольственная безопасность

Original article

CYBERSECURITY IN THE RUSSIAN AGRO-INDUSTRIAL COMPLEX: TOOLS, CASES, INCIDENTS

D.M. Nazarov[1], Yu.V. Gudoshnikova[1], N.V. Serbina[1], N.G. Protas[2]

[1]Ural State University of Economic, Ekaterinburg, Russia
[2]Novosibirsk State University of Economics and Management, Novosibirsk, Russia

Abstract. The relevance of this study stems from the rapid digitalisation of Russia's agro-industrial complex and the growing dependence of the sector on information systems, industrial control systems and governmental traceability platforms. Cyber incidents in agriculture are no longer a purely IT issue: recent attacks against large agribusiness groups, logistics hubs, processing plants and state information systems have affected physical production, cold-chain infrastructure and export flows. These cases demonstrate a shift of cyber risks from data confidentiality to operational resilience and food security. The purpose of the paper is to systematise the cyber-threat landscape for the Russian agro-industrial complex, to describe dominant attack scenarios, and to analyse the cybersecurity tools and risk-management standards used in practice, assessing their suitability for sector-specific conditions. Methodologically, the research relies on qualitative analysis of scientific literature on agricultural cybersecurity and digital agriculture, international industry reports on cyber threats to the food and agriculture sector, Russian media and industry case studies of cyberattacks, and official regulatory documents governing the protection of critical information infrastructure and governmental information systems. The novelty of the paper lies in the integrated linkage of three analytical levels: global statistics on attacks against the food and agriculture sector, publicly reported Russian incidents in agro-industrial chains, and real-world implementations of sector-specific cybersecurity solutions. The study proposes a structured matrix connecting incident types along the "farm — processing — logistics — control and traceability" chain with clusters of security tools (SOC/SIEM, EDR/XDR, OT/IoT security, IRP/SOAR, DLP/DCAP) and risk-management frameworks (ISO/IEC 27001, NIST CSF 2.0, Russian critical-infrastructure regulations). As a result, an industry-oriented "minimal standard" of cyber-resilience is outlined that reflects the specificity of Russian agribusiness and state digital platforms.

Keywords: cyber incidents, critical information infrastructure, cyber risk management, food security

Постановка проблемы. За последнее десятилетие агропромышленный комплекс России демонстрирует устойчивый рост цифровой интенсивности: внедряются системы точного земледелия, автоматизированные комплексы животноводства, платформы управления логистикой и экспортом, государственные информационные системы прослеживаемости и контроля качества. Эти изменения структурируют новый профиль рисков: отказ информационных систем и искажение данных становятся источником прямых потерь урожая, сбоев логистики и нарушения обязательств перед сетевыми ритейлерами и экспортными партнёрами. В мировой литературе подчёркивается, что современное сельское хозяйство превращается в высокотехнологичную отрасль, тесно связанную с цифровыми платформами, сенсорными сетями и аналитикой больших данных [1, 5, 8]. Параллельно растёт зависимость продовольственной безопасности от устойчивости цифровой инфраструктуры, что делает киберриски компонентой экономической и продовольственной безопасности государства [3, 6, 9, 13]. Для России, где АПК играет ключевую роль в экспортной и региональной повестке, эта взаимосвязь усиливается структурной ролью государства, высокой долей инфраструктуры, относимой к критической информационной, и наличием распределённых активов в удалённых территориях. Практика показывает, что аграрный сектор перестал быть «второстепенной» целью злоумышленников. Исследовательские центры и отраслевые ISAC-структуры фиксируют резкий рост атак на продовольственный и аграрный сектор: только за первые три месяца 2025 года за рубежом было зафиксировано 84 атаки вымогательского ПО на организации продовольственной и аграрной отрасли — более чем вдвое больше, чем годом ранее. Российские аналитические обзоры [17, 18] отмечают сопоставимый тренд: доля целенаправленных атак на АПК растёт и сопровождается увеличением сложности сценариев, включая использование уязвимостей в цепочке поставок и компрометацию подрядчиков. В российском контексте особое значение приобретает пересечение трёх контуров: корпоративной цифровой инфраструктуры

агрохолдингов; технологических систем (АСУ ТП, датчики, телематика, холодильное оборудование); государственных информационных систем в сфере контроля и прослеживаемости.

Аварийный режим работы ФГИС «ВетИС» в июне 2025 года, вызванный вирусной атакой, показал, что дестабилизация государственных платформ способна в короткий срок создать операционные сложности у широкого круга участников цепочки поставок: оформление сопроводительных документов было временно переведено на бумажные носители, что увеличило транзакционные издержки и риски ошибок [19]. Одновременно ряд крупных российских агрохолдингов столкнулся с масштабными атаками шифровальщиков, затронувшими практически все ИТ-системы компании и сопровождавшимися вымогательством значительных сумм. Масштабная кибератака на «Агрокомплекс им. Н.И. Ткачева» в апреле 2024 года сопровождалась похищением и шифрованием данных и требованием выкупа порядка 500 млн руб., при этом восстановление работы инфраструктуры заняло несколько дней, хотя компании удалось сохранить непрерывность поставок для населения и партнёров [2]. Ранее аналогичный характер носила атака на производственные информационные системы Ростовского колбасного завода «Тавр», где вредоносное ПО затронуло серверы, рабочие станции и ключевые бизнес-приложения, что фактически было оценено как диверсия против предприятия пищевой промышленности. Эти случаи демонстрируют переход киберинцидентов из сферы «неудобств» (потеря части офисных данных) в сферу реальных угроз непрерывности производства, сохранности продукции и продовольственной безопасности.

Нормативная база России реагирует на эти вызовы через развитие законодательства о безопасности критической информационной инфраструктуры. Федеральный закон № 187-ФЗ закрепляет обязанности субъектов КИИ по обеспечению устойчивого функционирования значимых объектов, а приказ ФСТЭК России № 239 детализирует требования к безопасности значимых объектов КИИ на всех этапах жизненного цикла. Однако перевод этих требований в операционные практики агрокомпаний требует адаптации к специфике сезонности, территориальной распределённости и высокой доли аутсорсинговых сервисов.

Международные стандарты управления киберриском, прежде всего NIST Cybersecurity Framework 2.0, обновлённый в феврале 2024 года, предлагают универсальную архитектуру, основанную на шести функциях: Govern, Identify, Protect, Detect, Respond, Recover [4]. Применительно к АПК это позволяет связать технологические меры (SIEM/SOC, EDR, сегментация OT-сетей, резервное копирование) с управленческими решениями (определение «недопустимых событий», приоритизация рисков, метрики зрелости) [7].

Таким образом, складывается несколько исследовательских разрывов. Во-первых, недостаточно системных работ, сочетающих глобальный взгляд на киберриски в сельском хозяйстве с российской нормативной и институциональной спецификой. Во-вторых, пока ограничен массив эмпирических данных по реальному уровню внедрения средств защиты в российских предприятиях АПК, особенно на уровне средних и малых хозяйств. В-третьих, требуется разработка понятной для управленцев типологии инцидентов, отражающей переход угроз в технологический контур и позволяющей выстроить приоритеты инвестиций в кибербезопасность.

Исследования кибербезопасности в сельском хозяйстве формируются на стыке трёх научных полей: информационной безопасности [10], аграрной экономики и теории продовольственной безопасности [11]. На нормативном уровне вопросы безопасности критической информационной инфраструктуры России регулируются федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [20]. Требования к безопасности значимых объектов КИИ детализируются приказом ФСТЭК России № 239, который охватывает этапы создания, эксплуатации и вывода из эксплуатации объектов [21]. На международном уровне стандартизация подходов к управлению киберриском развивается на основе NIST Cybersecurity Framework 2.0, предлагающего универсальную архитектуру для различных отраслей экономики [22].

Анализ литературы позволяет сделать несколько выводов. Во-первых, мировой научный дискурс уже признаёт сельское хозяйство частью критической инфраструктуры и рассматривает киберриски как компонент продовольственной безопасности. Во-вторых, в российской литературе активно обсуждаются вопросы цифровизации АПК и развития аграрной науки, но проблематика кибербезопасности пока представлена фрагментарно и преимущественно в прикладных, а не теоретико-методологических публикациях. В-третьих, нормативная база КИИ и международные стандарты управления киберрисками создают рамку для формирования комплексных программ киберзащиты, однако специфические особенности аграрного сектора (сезонность, территориальная распределённость, сильная зависимость от государственной цифровой инфраструктуры) остаются недостаточно интегрированными в эти рамки.

Цель исследования — систематизировать ландшафт киберугроз для агропромышленного комплекса России, описать доминирующие сценарии атак и проанализировать применяемые инструменты кибербезопасности и стандарты управления рисками с точки зрения их соответствия отраслевой специфике.

Методология и методы исследования. Методологической основой работы является междисциплинарный подход, объединяющий экономику сельского хозяйства, теорию управления рисками и современные концепции кибербезопасности и киберустойчивости.

Использована научная литература по цифровизации сельского хозяйства, продовольственной и экономической безопасности, а также по киберрискам в аграрных и продовольственных цепочках. В эту группу входят работы по кибербезопасности в сельском хозяйстве и пищевой промышленности, исследования угроз цифровым платформам и обзоры тенденций развития кибербезопасности.

Проанализированы международные отраслевые отчёты и аналитические записки профильных ассоциаций и центров мониторинга угроз. Особое значение имеет ежегодная статистика Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC) по атакам программ-вымогателей на пищевую и аграрную отрасли, где фиксируется рост числа инцидентов и доли данного сектора в общем объёме кибератак на критически важные отрасли.

Систематизированы российские открытые источники: материалы отраслевых медиа о кибератаках на агрохолдинги и перерабатывающие предприятия, публикации о взломе агрологистического хаба «Селятино», официальные сообщения Россельхознадзора об аварийном режиме работы ФГИС «ВетИС» и о DDoS-атаках на государственные информационные системы, а также интервью и аналитика единого центра цифровизации АПК «Агропромцифра» и ИБ-интеграторов, реализующих проекты для аграрных компаний.

Результаты. За последние годы продовольственный и аграрный сектор становится одной из приоритетных целей для киберпреступников на глобальном уровне. Отраслевые обзоры Food and Ag-ISAC фиксируют устойчивый рост атак программ-вымогателей на компании цепочки «от фермы до стола» и подчёркивают, что пищевая и аграрная отрасли стабильно входят в число наиболее атакуемых критически важных секторов по числу инцидентов и их темпам роста.

Использована научная литература по цифровизации сельского хозяйства, продовольственной и экономической безопасности, а также по киберрискам в аграрных и продовольственных цепочках. В эту группу входят работы по кибербезопасности в сельском хозяйстве и пищевой промышленности, исследования угроз цифровым платформам и обзоры тенденций развития кибербезопасности.

Проанализированы международные отраслевые отчёты и аналитические записки профильных ассоциаций кибербезопасности и киберустойчивости. В российских условиях этот фон усиливается спецификой цифровой инфраструктуры: высокими требованиями к прослеживаемости, централизацией государственных сервисов («ВетИС», «Меркурий», «Сатурн») и быстрым внедрением цифровых решений на уровне крупных агрохолдингов и переработки (табл. 1).

Сопоставление глобальных и российских данных свидетельствует о трансформации аграрного сектора в устойчиво атакуемый сегмент

Таблица 1. **Показатели киберугроз для аграрного и продовольственного сектора**
Table 1. **Indicators of cyber threats to the agricultural and food sectors**

Показатель	Значение	География и период
Доля атак программ-вымогателей, пришедшихся на пищевую и аграрную отрасли в первом квартале 2025 года	5,5% от общего числа инцидентов, 84 атаки	Глобальный сектор food & agriculture, I кв. 2025 г.
Число атак программ-вымогателей на food & agriculture за год	265 инцидентов, около 4,2% от всех атак по отраслям критической инфраструктуры	Глобальный сектор food & agriculture, 2025 г.
Оценка целенаправленных кибератак на предприятия АПК России	более 1 тыс. целевых атак за год	Россия, предприятия АПК, 2025 г.
Общее количество кибератак по российскому сегменту Интернет за полугодие и доля объектов КИИ	десятки тысяч атак, при этом значительная часть направлена на объекты критической информационной инфраструктуры	Россия, совокупность отраслей, полугодовой период наблюдения

Составлено авторами по: [6, 11, 19, 20, 22]

критической инфраструктуры. На международном уровне отрасль демонстрирует стабильное присутствие в статистике программ-вымогателей и рост числа инцидентов. В России значимым индикатором становится не только количество целевых атак, но и увеличение доли АПК в общем массиве киберинцидентов. Высокая роль социальной инженерии подчёркивает зависимость сектора от организационных мер, подготовки персонала и контроля удалённого доступа. Существенное значение имеют DDoS-атаки на государственные цифровые сервисы, поскольку перебои в их работе напрямую затрагивают логистику и прослеживаемость продукции.

Практика показывает, что инциденты охватывают все звенья продовольственной цепочки — от технологического оборудования до государственных платформ. Для эффективного управления рисками необходима их систематизация по объектам воздействия, типам угроз и последствиям для бизнеса и государства (табл. 2).

Представленная типология показывает, что киберугрозы для АПК охватывают три взаимосвязанных уровня. Первый — технологическая инфраструктура хранения и переработки, где воздействие на системы управления способно вызвать остановку производственных линий и риски порчи продукции. Второй — корпоративные ИТ-системы агрохолдингов: атаки программ-вымогателей приводят к блокировке данных, утечкам информации и срочному восстановлению процессов. Третий — государственные платформы прослеживаемости и контроля, где DDoS- и вирусные атаки нарушают сертификацию и документооборот, увеличивая операционные издержки.

Общим следствием инцидентов становится пересмотр управленческих практик: усиление мониторинга, сегментация сетей, ограничение удалённого доступа и развитие планов непрерывности бизнеса. Российские компании демонстрируют поэтапное повышение зрелости — от базовых мер защиты к формированию комплексных архитектур с центрами мониторинга, специализированной защитой промышленных сетей и автоматизацией реагирования, интегрируя требования национального регулирования и международных стандартов в практику управления киберрисками. (табл. 3).

Систематизация инструментов показывает, что в российском АПК складывается архитектура кибербезопасности, соответствующая лучшим практикам управления киберрисками, но адаптированная к отраслевой специфике. Кластеры SOC/SIEM и IRP/SOAR обеспечивают управляемую «надстройку» над множеством технических средств, позволяя агрохолдингам переходить от реакции «по факту» к непрерывному мониторингу и формализованному реагированию. EDR/XDR и защита конечных точек становятся необходимым минимумом, без которого невозможно противостоять атакам программ-вымогателей, тогда как OT-security и сегментация промышленных сетей являются ответом на риск вмешательства в технологические процессы, наглядно проявившийся в кейсе агрохаба «Селятино». Проактивный детект сложных угроз и программы аудитов и пентестов позволяют смещать акцент с постфактум расследований на раннее выявление и снижение экспозиции к рискам, что особенно важно в условиях роста числа целевых атак на АПК.

Заключение. Проведённое исследование подтверждает, что агропромышленный комплекс и продовольственные цепочки закрепляются среди приоритетных целей киберпреступников как на глобальном, так и на национальном уровнях. В российском контексте дополнительным фактором уязвимости выступает зависимость отрасли от государственных цифровых платформ прослеживаемости и контроля, что придаёт киберрискам измерение продовольственной и экономической безопасности.

Типология инцидентов выявляет их «сквозной» характер: угрозы затрагивают одновременно OT/IoT-контуры, корпоративные ИТ-системы и государственные сервисы. Нарушение одного звена способно вызвать каскадные эффекты в логистике и производстве. Анализ практик российских компаний демонстрирует переход к комплексным архитектурам киберзащиты, ориентированным на операционную устойчивость и непрерывность агропроизводства. Сопоставление с международными и национальными стандартами позволило сформулировать минимальный отраслевой стандарт киберустойчивости.

Таблица 2. **Киберинциденты, затрагивающие российский АПК и продовольственные цепочки**
Table 2. **Cyber incidents affecting the Russian agro-industrial complex and food chains**

Год	Объект	Тип кибер-воздействия	Последствия
2022	Агрологистический хаб «Селятино» (холодильные мощности)	Взлом оборудования управления холодильными установками	Злоумышленники получили удалённый доступ к системе управления морозильным цехом и пытались изменить температурный режим, под угрозой оказалось около 40 тыс. тонн замороженной мясной и рыбной продукции; служба безопасности восстановила корректные параметры и предотвратила порчу продукции
2024	Агрокомплекс им. Н.И. Ткачева (крупный агрохолдинг)	Масштабная атака с использованием вируса-шифровальщика на все ИТ-системы	Поражение всех ИТ-систем, кража данных с серверов, выдвижение требования выкупа в размере сотен миллионов рублей; компания сообщала о техническом сбое, вызванном атакой, и о планах восстановить операционную деятельность в течение нескольких дней, подчёркивая отсутствие влияния на поставки продукции
2025	ФГИС «ВетИС» (компонент «Меркурий»)	Вирусная атака и перевод системы в аварийный режим	Официально объявленный аварийный режим работы компонента «Меркурий», временная недоступность электронного оформления ветеринарных сопроводительных документов, переход на бумажные процедуры и последующее поэтапное восстановление web- и API-доступа в течение нескольких недель; формальное завершение аварийного режима в июле 2025 года
2025	Информационные системы Россельхознадзора («ВетИС», «Сатурн»)	Масштабная DDoS-атака	С 8:40 22 октября 2025 года фиксировалась масштабная целенаправленная DDoS-атака на основные информационные ресурсы службы; сообщалось о возможной временной недоступности сервисов и нестабильности каналов, при этом подчёркивалось отсутствие угроз целостности и конфиденциальности данных и принятие исчерпывающих мер по защите

Составлено авторами по: [7, 15, 21, 22]

Таблица 3. **Кластеры инструментов кибербезопасности**
Table 3. **Clusters of cybersecurity tools**

Кластер решений	Основное назначение в контексте АПК
SOC/SIEM и централизованный мониторинг	Сбор и корреляция событий ИБ из распределённой инфраструктуры агрохолдинга, выявление атак на корпоративные и промышленные сегменты, координация реагирования, формирование метрик зрелости и «здоровья» контуров безопасности
EDR/XDR и защита конечных точек	Предотвращение распространения вредоносного ПО и программ-вымогателей на рабочих станциях и серверах, быстрая изоляция скомпрометированных узлов, восстановление целостности систем
OT-security и сегментация промышленных сетей	Обнаружение и предотвращение вмешательства в АСУ ТП, системы управления холодильными установками, технологическими линиями и инженерной инфраструктурой; сегментация IT/OT, мониторинг отраслевых протоколов
IRP/SOAR и автоматизация реагирования	Формализация сценариев реагирования, автоматическое создание задач и сбор артефактов, интеграция с внешними SOC и корпоративными системами (AD, CMDB, антивирус, HR), сокращение времени реакции
Проактивный детект сложных угроз	Поиск и блокирование сложных и ранее неизвестных угроз, таргетированных атак и вредоносных рассылок до их влияния на производственные процессы
Аудиты, пентесты и программы киберустойчивости	Регулярная переоценка уязвимостей, проверка устойчивости периметра и внутренних сегментов, выработка дорожных карт повышения зрелости, тестирование готовности к инцидентам

Составлено авторами по: [19-22]

Список источников

1. Alahmadi, A.N., Rehman, S. ur., Alhazmi, H.S., Glynn, D.G., Shoaib, H., Solé, P. Cyber-security threats and side-channel attacks for digital agriculture // Sensors. 2022. Vol. 22, No. 9. P. 3520. DOI: 10.3390/s22093520. EDN XHSBWG.

2. Benzel, T. Cybersecurity research for the future // Communications of the ACM. 2021. Vol. 64, No. 1. P. 26–28. DOI: 10.1145/3436241. EDN KEKNOO.

3. Chen, N., Li, H. Agricultural economic security under the model of integrated agricultural industry development // Quality Assurance and Safety of Crops and Foods. 2024. Vol. 16, No. 3. P. 25–41. DOI: 10.15586/qas.v16i3.1470. EDN TMNPXT.

4. Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R.S., Duncan, S.E. Assessing the role of cyberbiosecurity in agriculture: A case study // Frontiers in Bioengineering and Biotechnology. 2021. Vol. 9. DOI: 10.3389/fbioe.2021.737927. EDN JJYLMR.

5. Giua, C., Materia, V.C., Camanzi, L. Smart farming technologies adoption: Which factors play a role in the digital transition? // Technology in Society. 2022. Vol. 68. P. 101869. DOI: 10.1016/j.techsoc.2022.101869. EDN RLIBSY.

6. Guiné, R.P. F. The challenges and strategies of food security under global change // Foods. 2024. Vol. 13, No. 13. P. 2083. DOI: 10.3390/foods13132083. EDN FQWZKZ.

7. Kamarudin, S., Tang, L., Bolong, J., Adzharuddin, N.A. A systematic literature review of mitigating cyber security risk // Quality and Quantity. 2023. DOI: 10.1007/s11135-023-01791-9. EDN FGXSNY.

8. Khatri, P., Kumar, P., Shakya, K.S., Kirlas, M.C., Tiwari, K.K. Understanding the intertwined nature of rising multiple risks in modern agriculture and food system // Environment, Development and Sustainability. 2023. DOI: 10.1007/s10668-023-03638-7. EDN BDQIMR.

9. McCreight, R. Agricultural security: Critical national infrastructure we cannot ignore // Journal of Homeland Security and Emergency Management. 2022. Vol. 19, No. 1. P. 127–135. DOI: 10.1515/jhsem-2021-0077. EDN ZRVTNT.

10. Morris, G., Ehlers, Sh., Aaltonen, P.M., Sheldon, E., Johnson, A. Review of livestock biosecurity resources and trainings: Local, state, federal, and international organizations // Journal of Biosafety and Biosecurity. 2023. Vol. 5, No. 4. P. 162–169. DOI: 10.1016/j.jobb.2023.12.001. EDN FQOZAA.

11. Pöysti, T. Governance of societal cyber and information security risks // Jusletter IT. 2023. No. 23-Februar-2023. DOI: 10.38023/1a8abe46-9b7f-452f-ad2a-6a4adc09d22a. EDN TXJTSI.

12. Saboori, B., Radmehr, R., Zhang, Y.Y., Zekri, S. A new face of food security: A global perspective of the COVID-19 pandemic // Progress in Disaster Science. 2022. Vol. 16. P. 100252. DOI: 10.1016/j.pdisas.2022.100252. EDN OADHQX.

13. Seppelt, R., Klotz, S., Peiter, E., Volk, M. Agriculture and food security under a changing climate: An underestimated challenge // iScience. 2022. Vol. 25, No. 12. P. 105551. DOI: 10.1016/j.isci.2022.105551. EDN KJXVPK.

14. Shigeaki, S. The essential challenge of "economic security" // Asia-Pacific Review. 2022. Vol. 29, No. 3. P. 78–91. DOI: 10.1080/13439006.2022.2154508. EDN XRELCK.

15. Stephen, S., Ruffin, D., Palmer, X., Potter, L. Securing agricultural systems against the threat of misinformation // Journal of the ASABE. 2024. Vol. 67, No. 6. P. 1595–1605. DOI: 10.13031/ja.15979. EDN RAMAST.

16. Teichmann, F., Boticiu, S., Sergi, B.S. Cybersecurity trends in 2023 // Jusletter IT. 2022. No. 20-Dezember-2022. DOI: 10.38023/8e17cdc3-b9b9-463c-b993-685bf6cc12ad. EDN SUDKPA.

17. Валиев, А.Р., Низамов, Р.М., Сафин, Р.И., Мухаметгалиев, Ф.Н., Нежметдинова, Ф.Т. Приоритеты развития агропромышленного комплекса и задачи аграрной науки и образования // Вестник Казанского государственного аграрного университета. 2022. Т. 17, № 1(65). С. 97–107. DOI :10.12737/2073-0462-2022-97-107. EDN BFQMKB.

18. Кондратьева, О.В., Федоров, А.Д., Слинько, О.В., Войтюк, В.А. Совершенствование информационных технологий в отечественном АПК // Техника и оборудование для села. 2023. № 8(314). С. 7–11. DOI: 10.33267/2072-9642-2023-8-7-11. EDN SVAXAV.

19. Назаров, Д.М., Кондратенко, И.С., Сулимин, В.В., Шведов, В.В. Цифровизация сельского хозяйства на примере Румынии // Международный сельскохозяйственный журнал. 2022. № 6(390). С. 622–624. DOI: 10.55186/25876740_2022_65_6_622. EDN KEQEIC.

20. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ (ред. от 10.07.2023). URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 08.12.2025).

21. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25 дек. 2017 г. № 239 (ред. от 28.08.2024). URL: http://docs.cntd.ru/document/542612884 (дата обращения: 08.12.2025).

22. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 // NIST Cybersecurity White Paper. 2024. 29 p. (NIST CSWP 29). URL: http://www.nist.gov/cyberframework (accessed: 08.12.2025).

References

1. Alahmadi, A.N., Rehman, S. ur., Alhazmi, H.S., Glynn, D.G., Shoaib, H., Solé, P. Cyber-security threats and side-channel attacks for digital agriculture // Sensors. 2022. Vol. 22, No. 9. P. 3520. DOI: 10.3390/s22093520. EDN XHSBWG.

2. Benzel, T. Cybersecurity research for the future // Communications of the ACM. 2021. Vol. 64, No. 1. P. 26-28. DOI: 10.1145/3436241. EDN KEKNOO.

3. Chen, N., Li, H. Agricultural economic security under the model of integrated agricultural industry development // Quality Assurance and Safety of Crops and Foods. 2024. Vol. 16, No. 3. P. 25-41. DOI: 10.15586/qas.v16i3.1470. EDN TMNPXT.

4. Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R.S., Duncan, S.E. Assessing the role of cyberbiosecurity in agriculture: A case study // Frontiers in Bioengineering and Biotechnology. 2021. Vol. 9. DOI: 10.3389/fbioe.2021.737927. EDN JJYLMR.

5. Giua, C., Materia, V.C., Camanzi, L. Smart farming technologies adoption: Which factors play a role in the digital transition? // Technology in Society. 2022. Vol. 68. P. 101869. DOI: 10.1016/j.techsoc.2022.101869. EDN RLIBSY.

6. Guiné, R.P. F. The challenges and strategies of food security under global change // Foods. 2024. Vol. 13, No. 13. P. 2083. DOI: 10.3390/foods13132083. EDN FQWZKZ.

7. Kamarudin, S., Tang, L., Bolong, J., Adzharuddin, N.A. A systematic literature review of mitigating cyber security risk // Quality and Quantity. 2023. DOI: 10.1007/s11135-023-01791-9. EDN FGXSNY.

8. Khatri, P., Kumar, P., Shakya, K.S., Kirlas, M.C., Tiwari, K.K. Understanding the intertwined nature of rising multiple risks in modern agriculture and food system // Environment, Development and Sustainability. 2023. DOI: 10.1007/s10668-023-03638-7. EDN BDQIMR.

9. McCreight, R. Agricultural security: Critical national infrastructure we cannot ignore // Journal of Homeland Security and Emergency Management. 2022. Vol. 19, No. 1. P. 127-135. DOI: 10.1515/jhsem-2021-0077. EDN ZRVTNT.

10. Morris, G., Ehlers, Sh., Aaltonen, P.M., Sheldon, E., Johnson, A. Review of livestock biosecurity resources and trainings: Local, state, federal, and international organizations // Journal of Biosafety and Biosecurity. 2023. Vol. 5, No. 4. P. 162-169. DOI: 10.1016/j.jobb.2023.12.001. EDN FQOZAA.

11. Pöysti, T. Governance of societal cyber and information security risks // Jusletter IT. 2023. No. 23-Februar-2023. DOI: 10.38023/1a8abe46-9b7f-452f-ad2a-6a4adc09d22a. EDN TXJTSI.

12. Saboori, B., Radmehr, R., Zhang, Y.Y., Zekri, S. A new face of food security: A global perspective of the COVID-19 pandemic // Progress in Disaster Science. 2022. Vol. 16. P. 100252. DOI: 10.1016/j.pdisas.2022.100252. EDN OADHQX.

13. Seppelt, R., Klotz, S., Peiter, E., Volk, M. Agriculture and food security under a changing climate: An underestimated challenge // iScience. 2022. Vol. 25, No. 12. P. 105551. DOI: 10.1016/j.isci.2022.105551. EDN KJXVPK.

14. Shigeaki, S. The essential challenge of "economic security" // Asia-Pacific Review. 2022. Vol. 29, No. 3. P. 78-91. DOI: 10.1080/13439006.2022.2154508. EDN XRELCK.

15. Stephen, S., Ruffin, D., Palmer, X., Potter, L. Securing agricultural systems against the threat of misinformation // Journal of the ASABE. 2024. Vol. 67, No. 6. P. 1595-1605. DOI: 10.13031/ja.15979. EDN RAMAST.

16. Teichmann, F., Boticiu, S., Sergi, B.S. Cybersecurity trends in 2023 // Jusletter IT. 2022. No. 20-Dezember-2022. DOI: 10.38023/8e17cdc3-b9b9-463c-b993-685bf6cc12ad. EDN SUDKPA.

17. Valiev, A.R., Nizamov, R.M., Safin, R.I., Mukhametgaliev, F.N., Nezhmetdinova, F.T. (2022). *Prioritety razvitiya agropromyshlennogo kompleksa i zadachi agrarnoy nauki i obrazovaniya* [Priorities for the development of the agro-industrial complex and tasks of agrarian science and education]. *Vestnik Kazanskogo gosudarstvennogo agrarnogo universiteta* [Bulletin of Kazan State Agrarian University], vol. 17, no. 1(65). P. 97-107. DOI: 10.12737/2073-0462-2022-97-107. EDN BFQMKB.

18. Kondratyeva, O.V., Fedorov, A.D., Slinko, O.V., Voytyuk, V.A.(2023). Sovershenstvovanie informatsionnykh tekhnologii v otechestvennom APK [Improvement of information technologies in the domestic agro-industrial complex]. *Tekhnika i oborudovanie dlya sela* [Machinery and Equipment for Rural Area], no. 8(314), p. 7-11. DOI: 10.33267/2072-9642-2023-8-7-11. EDN SVAXAV.

19. Nazarov, D.M., Kondratenko, I.S., Sulimin, V.V., Shvedov, V.V. (2022). *Tsifrovizatsiya selskogo khozyaystva na primere Rumynii* [Digitalization of agriculture on the example of Romania]. *Mezhdunarodnyy selskokhozyaystvennyy zhurnal,* no. 6(390), p. 622-624. DOI: 10.55186/25876740_2022_65_6_622. EDN KEQEIC.

20. *O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Federal'nyj zakon* № 187-FZ ot 26 *iyulya* 2017 g. (red. ot 10.07.2023). Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/ (accessed 08 December 2025).

21. *Ob utverzhdenii Trebovanij po obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Prikaz FSTEK Rossii* № 239 ot 25 *dekabrya* 2017 g. (red. ot 28.08.2024). Available at: http://docs.cntd.ru/document/542612884 (accessed 08 December 2025).

22. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper. 2024, 29 p. (NIST CSWP 29). Available at: http://www.nist.gov/cyberframework (accessed 08 December 2025).

Информация об авторах:

Назаров Дмитрий Михайлович, доктор экономических наук, заведующий кафедрой бизнес-информатики, заведующий кафедры информационной безопасности, Уральский государственный экономический университет, ORCID: http://orcid.org/0000-0002-5847-9718, slup20005@mail.ru

Гудошникова Юлия Викторовна, кандидат экономических наук, доцент кафедры финансов, денежного обращения и кредита, Уральский государственный экономический университет, ORCID: http://orcid.org/0009-0000-2385-3370, YKuvaeva1974@mail.ru

Сербина Наталия Витальевна, кандидат искусствоведения, доцент кафедры экономики труда и управления персоналом, Уральский государственный экономический университет, ORCID: http://orcid.org/0000-0002-6475-0631, serbina_nv@usue.ru

Протас Нина Геннадьевна, кандидат экономических наук, доцент, заведующий финансового рынка и финансовых институтов, Новосибирский государственный университет экономики и управления, ORCID: http://orcid.org/0000-0002-4042-1593, n.protas1@mail.ru

Information about the authors:

Dmitry M. Nazarov, doctor of economics, head of the department of business informatics, Ural state economic university, ORCID: http://orcid.org/0000-0002-5847-9718, slup20005@mail.ru

Yulia V. Gudoshnikova, candidate of economic sciences, associate professor of the department of finance, money circulation and credit, Ural state economic university, ORCID: http://orcid.org/0009-0000-2385-3370, YKuvaeva1974@mail.ru

Natalia V. Serbina, candidate in art sciences, associate professor of the department of labor economics and personnel management, ORCID: http://orcid.org/0000-0002-6475-0631, serbina_nv@usue.ru

Nina G. Protas, candidate of economic sciences, associate professor, head of the financial market and financial institutions, Novosibirsk state university of economics and management, ORCID: http://orcid.org/0000-0002-4042-1593, n.protas1@mail.ru

✉ **slup20005@mail.ru**