ЦИФРОВАЯ ЭКОНОМИКА

УДК: 338.1
JEL: O13

Оценка восприятия проблем информационной безопасности предприятиями АПК при переходе к умному сельскому хозяйству

А.А. Иванова
https://orcid.org/0009-0007-3055-6068
e-mail: *nasty.ivanova-05@mail.ru*

А.Я. Киленников
https://orcid.org/0009-0007-7871-9524; SPIN-код (РИНЦ): 8806-4218
e-mail: *akilennikov@mail.ru*

И.М. Степнов, д.э.н., профессор
https://orcid.org/0000-0003-4107-6397; SPIN-код (РИНЦ): 3806-1500
Scopus author ID: 57192089541
e-mail: *stepnoff@inbox.ru*

Для цитирования
Иванова А.А., Киленников А.Я., Степнов И.М. Оценка восприятия проблем информационной безопасности предприятиями АПК при переходе к умному сельскому хозяйству // Проблемы рыночной экономики. – 2026. – № 3. – С. 173-189.
DOI: 10.33051/2500-2325-2026-3-173-189

Аннотация
Статья посвящена результатам выборочного опроса предприятий российского агропромышленного комплекса, проведенного с целью установления восприятия руководством таких предприятий существенности угроз информационной безопасности. Показано, что декларируемый переход к умному сельскому хозяйству сопровождается не только ростом производительности труда, но и нарастанием рисков, прежде всего, информационных. Используемый в исследовании подход методологически опирается на тот факт, что особенностью сельского хозяйства и АПК в сфере безопасности является способность быстрого перехода от цифрового сбоя к биологическим, производственным и экономическим потерям. Аргументировано, что появление цифровых технологий, присущих концепции умного сельского хозяйства, несмотря на осведомленность руководства предприятий о рисках такого перехода, требует дополнительных мер по обеспечению информационной безопасности. Это подтверждено результатами выборочного исследования (в рамках первичной апробации подхода) в рамках анкетирования восприятия угроз отдельными предприятиями АПК различных организационно-правовых форм и форм собственности (ООО, ИП, крестьянско-фермерское хозяйство, НПАО) из Волгоградской, Воронежской и Саратовской областей Российской Федерации. Полученные результаты позволили сделать обоснованный вывод о необходимости более широкого исследования для понимания истинного размера киберугроз в цифровизируемом сельском хозяйстве, в том числе и для проектирования эффективной системы противостояния таким угрозам. Ценность исследования состоит в систематизации результатов опросов, которые позволили установить, что вероятность угроз предприятиям в сельском хозяйстве достаточно высока, в том числе и из недостаточного восприятия киберугроз в хозяйствах.

Ключевые слова: *сельское хозяйство, сельское хозяйство 4.0, умное сельское хозяйство, агропромышленный комплекс, цифровизация, риски, информационная безопасность.*

Assessment of the perception of information security issues by agro-industrial enterprises during the transition to smart agriculture

Anastasia A. Ivanova
https://orcid.org/0009-0007-3055-6068
e-mail: *nasty.ivanova-05@mail.ru*

Aleksandr Ya. Kilennikov
https://orcid.org/0009-0007-7871-9524; SPIN-code (RSCI): 8806-4218
e-mail: *akilennikov@mail.ru*

Igor M. Stepnov, Dr. of Sci. (Econ.), Professor
https://orcid.org/0000-0003-4107-6397; SPIN-code (RSCI): 3806-1500
Scopus author ID: 57192089541
e-mail: *stepnoff@inbox.ru*

For citation
Ivanova A.A., Kilennikov A.Ya, Stepnov I.M. Assessment of the perception of information security issues by agro-industrial enterprises during the transition to smart agriculture // Market economy problems. – 2026. – No. 3. – Pp. 173-189 (In Russian).
DOI: 10.33051/2500-2325-2026-3-173-189

Abstract
The article is devoted to the results of a sample survey of enterprises of the Russian agro-industrial complex, conducted in order to establish the perception of the materiality of threats to information security by the management of such enterprises. It is shown that the declared transition to smart agriculture is accompanied not only by an increase in labor productivity, but also by an increase in risks, primarily informational ones. The approach used in the study is methodologically based on the fact that a feature of agriculture and agriculture in the field of security is the ability to quickly transition from digital disruption to biological, industrial and economic losses. It is argued that the emergence of digital technologies inherent in the concept of smart agriculture, despite the awareness of the management of enterprises about the risks of such a transition, requires additional measures to ensure information security. This is confirmed by the results of a sample study (as part of the initial testing of the approach) as part of a survey of the perception of threats by individual agricultural enterprises of various organizational and legal forms and forms of ownership (limited liability companies, individual entrepreneurs, peasant farms, non-public joint-stock companies) from the Volgograd, Voronezh and Saratov regions of the Russian Federation. The results obtained allowed us to draw a reasonable conclusion about the need for a broader study to understand the true size of cyber threats in digitalized agriculture, including for designing an effective system to counter such threats. The value of the study lies in the systematization of the survey results, which made it possible to establish that the likelihood of threats to enterprises in agriculture is quite high, including due to insufficient perception of cyber threats in farms.

Keywords: *agriculture, agriculture 4.0, smart farming, agro-industrial complex, digitalization, risks, information security.*

Введение

Современный этап внедрения цифровых технологий в сельскохозяйственное производство и управление характеризуется все более ускоряющимися темпами проникновения информационных технологий как в международной, так и российской практике, сопровождаясь не только широким внедрением вычислительных систем, но GPS-навигации, дронов, датчиков влажности и температуры, систем спутникового мониторинга, технологий искусственного интеллекта, интернета вещей и др. [1, 11, 12]. Фактически сегодня простая автоматизация технологий сельского хозяйства позволяет наблюдать три стадии такого перехода: внедрение решений в рамках концепции сельского хозяйства 4.0, формирование подходов к реализации сельского хозяйства 5.0 [13] и одновременно реализации умного сельского хозяйства [2, 10] как точечных решений для конкретного предприятия АПК.

Внедрение технологий умного сельского хозяйства обещает значительное повышение производительности труда [3, 7] оптимизацию использования ресурсов и улучшение качества продукции: «сельское хозяйство на протяжении всего периода показывает лучший результат по этому показателю» – отмечают С.Ю. Глазьев и О.С. Сухарев [4, с. 14]. Однако одновременно с расширением применения цифровых решений в аграрном секторе возникают новые и ранее неизвестные угрозы информационной безопасности [9]. Новые технологии позволяют фермерам принимать обоснованные решения на основе больших объемов данных, но даже первые шаги в этом направлении одновременно создают новые векторы для киберугроз, так как такие решения требуют формирования взаимосвязанной среды: устройств, данных и внешних сервисов, доступа к интернету. Поэтому сельскохозяйственные предприятия становятся все более привлекательными целями для киберпреступников, поскольку часто обладают критически важными данными о производстве, финансовых операциях и логистике. Главная особенность киберрисков АПК – быстрый переход от цифрового сбоя к биологическим, производственным и экономическим потерям, в связи с тем, что быстрое восстановление информационной системы не всегда компенсирует последствия: пропущенный агротехнологический срок, гибель животных или порча продукции могут быть необратимыми.

Локальная работа информационных систем при традиционной автоматизации заменяется формированием взаимосвязанной среды при переходе к умному сельскому хозяйству:

- увеличивается число подключенных устройств. Каждый датчик, шлюз, контроллер или терминал становится объектом, который необходимо учитывать, обновлять и защищать;
- нарастает глубина интеграции корпоративных и производственных сетей. Инцидент в офисной инфраструктуре может распространиться на технологические системы при недостаточной сегментации;
- нарастает зависимость от внешних сервисов. Цифровая поддержка деятельности предприятия АПК может зависеть от облачных решений, мобильной связи, навигации, удалённой технической поддержки и механизмов лицензирования;
- все большее число участников включается в обмен данными. Агрономические, ветеринарные и производственные сведения передаются подрядчикам, аналитическим платформам и поставщикам оборудования;
- усложняется поддержка оборудования в течение всего жизненного цикла. Сельскохозяйственная техника может эксплуатироваться значительно дольше, чем поддерживается встроенное программное обеспечение.

Предпосылкой данного исследования стало утверждение, что, несмотря на то, что российский аграрный сектор находится на этапе активной цифровизации, уровень осведомленности сельскохозяйственных организаций о киберрисках остается недостаточным. Большинство хозяйств сосредоточены на получении преимуществ от новых технологий, уделяя меньше внимания вопросам информационной безопасности. Это создает критическую уязвимость в системе защиты стратегически важного сектора экономики.

Основные факторы уязвимости:

- территориальная распределенность, так как поля, фермы, склады и производственные площадки сложно защищать и обслуживать с одинаковым уровнем безопасности;
- дефицит специалистов, особенно у небольших и средних хозяйств, где IT-функции часто совмещены с другими обязанностями;

- устаревание используемого оборудования, так как часто контроллеры и встроенные процессоры могут не поддерживать современные механизмы аутентификации и обновления;
- ограниченные окна обслуживания, так как установка обновлений в сезон способна создать неприемлемый риск простоя;
- зависимость от интеграторов и производителей, так как небольшие предприятия не всегда контролируют удалённый доступ, журналы событий и сроки устранения уязвимостей;
- отсутствие полного реестра активов, так как подключённые устройства, сервисные модемы и облачные интеграции могут оставаться вне учёта;
- приоритет функциональности при закупках, когда зачастую кибербезопасность и возможность восстановления не всегда включаются в техническое задание.

С нашей точки зрения устранение таких уязвимостей на предприятиях АПК во многом связано с разным пониманием руководством истинных последствий киберугроз до наступления прецендента. Именно поэтому целью данного исследования является анализ взаимосвязи между внедрением технологий умного сельского хозяйства и возникновением новых киберрисков на основе практического исследования осведомленности об угрозах информационной безопасности в сельскохозяйственных организациях в ведущих агропромышленных областях Российской Федерации, включая реализацию таких задач, как:

- выявление основных факторов, препятствующих внедрению мер кибербезопасности;
- разработка рекомендаций по снижению киберрисков в условиях цифровизации сельского хозяйства.

Материалы и методы исследования

Для оценки состояния информационной безопасности в сельскохозяйственных организациях было проведено пробное анкетирование 18 сельскохозяйственных предприятий различных форм собственности (ООО, ИП, крестьянско-фермерские хозяйства, НПАО) из Волгоградской, Воронежской и Саратовской областей. Тест-анкета включала 27 вопросов, охватывающих следующие направления: использование цифровых технологий; контроль за выходом в Интернет; применяемые программные решения; практика столкновения с киберугрозами; информированность о киберрисках; мероприятия защиты данных; подготовленность к инвестициям в кибербезопасность; внутренние риски, связанные с человеческим фактором.

Размер исследованных хозяйств колебался от 600 до более 7000 гектаров обрабатываемой территории. Активная фаза исследования проводилась в период с мая по июль 2026 года.

Результаты

Согласно исследованию [5], можно выделить несколько наиболее значимых групп угроз: кража коммерчески значимой информации, включая сведения об урожайности, картах полей, логистических маршрутах, условиях контрактов и рецептурах кормов; шпионаж и промышленный саботаж, направленные на получение конкурентных преимуществ или нарушение деятельности предприятия; манипулирование данными, поступающими от датчиков и информационных систем отчетности, что может искажать управленческую картину и приводить к ошибочным решениям; а также атаки на системы управления сельскохозяйственной техникой и складской логистикой, способные вызвать остановку производственных процессов, сбои в снабжении и потери урожая.

Особую опасность данные угрозы представляют для собственников и руководителей агропромышленных предприятий, поскольку цифровизация отрасли находится на ранней стадии, а уровень распространенности специализированных средств киберзащиты остается сравнительно низким. В отличие от банковской сферы, где системы информационной безопасности развивались на протяжении многих лет, и сформировалась устойчивая практика противодействия инцидентам, в сельском хозяйстве многие цифровые решения внедряются сравнительно недавно и нередко используются без достаточного уровня защиты. Это создает дополнительную уязвимость для предприятий, повышая вероятность успешной реализации кибератак и усиливая риски для хозяйственной деятельности в целом.

Следует учитывать, что цифровизация АПК сама по себе является капиталоемким и продолжительным процессом, требующим значительных финансовых ресурсов и квалифицированных кадров. Ее внедрение осложняется исходно недостаточным уровнем развития цифровой инфраструктуры в сельской местности, ограниченной доступностью интернета в отдаленных районах, а также необходимостью модернизации оборудования, программного обеспечения и систем управления производством. В результате предприятия АПК сталкиваются не только с расходами на приобретение и настройку новых технологий, но и с дополнительными издержками на их интеграцию в уже существующие производственные процессы, обучение персонала и последующее техническое сопровождение.

Одной из важных причин цифровизации сельского хозяйства является сохраняющийся дефицит кадров [6]. Этот факт стимулирует государство и бизнес искать способы компенсации нехватки рабочей силы, в том числе за счет автоматизации процессов и внедрения искусственного интеллекта.

Технологии точного земледелия позволяют более эффективно контролировать густоту посевов, уровень засоренности полей и состояние растений. Применение беспилотных летательных аппаратов обеспечивает точечное внесение удобрений и средств защиты растений, что способствует снижению затрат и более рациональному использованию ресурсов. Данные, собираемые умными датчиками, анализируются с помощью ИИ, что дает возможность прогнозировать урожайность, выявлять болезни растений на ранних стадиях и своевременно принимать управленческие решения.

Современная сельскохозяйственная техника также все чаще оснащается интеллектуальными системами управления. Тракторы и комбайны с элементами ИИ способны работать в автоматизированном режиме, ориентируясь на спутниковую навигацию или системы технического зрения. Это позволяет технике точно определять свое положение, рассчитывать оставшуюся площадь обработки, а также прогнозировать затраты топлива и времени, повышая общую эффективность производственных операций [8, 9].

Для включения в опросы была проведена предварительная качественная систематизация угроз информационной безопасности, рассмотренных в доступных источниках, что позволило сгруппировать возможные угрозы следующим образом:

А: очень высокий риск:

- программы вымогатели (осуществляющие шифрование серверов, рабочих станций, систем учёта и связанных производственных сервисов), что приводит к простою, нарушению отгрузок, утрате доступа к производственным заданиям, и, в конечном счете, росту затрат;

- компрометация удаленного доступа (путем использования похищенной учётной записи сотрудника или подрядчика), что приводит к несанкционированному изменению настроек, остановке оборудования, проникновению в другие сегменты сети;

Б: высокий риск:

- нарушение целостности технологических данных (путем подмены показаний датчиков, производственных заданий, карт внесения или параметров кормления), что в итоге приводит к неверным управленческим решениям, перерасходу ресурсов, снижению урожайности и качества продукции;

- уязвимости устройств интернета вещей и контроллеров (из-за эксплуатации устаревшего ПО, типовых паролей или незащищённых интерфейсов), что приводит к потере контроля над устройствами и отказу мониторинга;

- физический доступ к устройствам (путем вмешательства в удалённые датчики, шкафы управления и шлюзы), что может привести к подмене измерений, повреждению оборудования, получение доступа к сети;

- атаки через поставщиков (из-за компрометации сервисной организации, обновления ПО или интеграционного сервиса), что приводит к одновременному поражению нескольких площадок и последующему длительному восстановлению;

В: средний риск:

- недоступность облачных платформ и связи (из-за DDoS-атак, блокировки учётной записи, сбоя внешнего сервиса), что приводит к потере диспетчеризации;

- нарушение навигации (вследствие подмены навигационных сигналов или организации радиопомех), что приводит к ошибкам позиционирования, пропускам обработки и остановка автоматического движения;

- утечка данных (в том числе, несанкционированное получение сведений об урожайности, себестоимости, земельных участках и контрагентах), что ведет к потере коммерческих преимуществ, мошенничеству и целому ряду правовых последствий;

- компрометация аналитики и моделей искусственного интеллекта (из-за возможности подмены входных данных или несанкционированного изменения модели), что приводит к ошибочности прогнозов и рекомендаций по поливу, защите растений или кормлению;

Отметим, что указание на уровень риска (очень высокий, высокий или средний) носит оценочный характер, так как каждое хозяйство будет выполнять собственное ранжирование рисков, но предложенный перечень угроз послужил основой для формирования опросов.

Следует отметить, что уровень цифровизации рассмотренных организаций существенно отличается, и только немного более половины активно используют вычислительную технику (только одно хозяйство указало, что практически не использует такую технику, несмотря на то, что было подтверждено, что компьютеры в этом хозяйств есть, и они обеспечены доступом в интернет) (рис.1). Однако практически 40% хозяйств, использующих компьютеры только выборочно, показывают на неполноценное внедрение цифровых решений в производственные процессы.

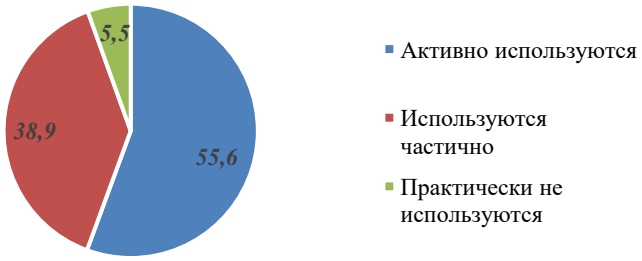

Рис. 1. Распределение сельскохозяйственных организаций по уровню использования компьютеров и ноутбуков, %

Источник: составлено авторами по результатам исследования.

Что касается доступа в интернет, положение еще более дифференцировано:

- 7 хозяйств (38,9%) предоставляют доступ в интернет большему числу работников;

- 11 хозяйств (61,1%) ограничивают доступ в интернет, предоставляя его только руководству и бухгалтерии.

Это говорит о том, что большинство аграрных организаций рассматривают интернет как инструмент управления и сопровождения финансовых операций, а не как способ для увеличения эффективности производства на уровне рядовых работников.

Применяемые цифровые устройства включают компьютеры (100% хозяйств), смартфоны (72,2%), GPS-навигаторы (61,1%), дроны (38,9%), датчики и сенсоры (22,2%), планшеты (11,1%). Следовательно, компьютеры остаются главным инструментом цифровизации, до настоящего времени символом цифровизации остаются компьютеры, в то время как более специальные устройства используются менее чем половиной исследованных хозяйств.

Информированность о разработках умного аграрного хозяйства среди исследованных организаций показана на рис. 2. Большинство аграрных предприятий (66,7%) имеют неглубокое ознакомление с концепцией умного аграрного хозяйства. Лишь четверть хозяйств (27,8%) хорошо разбираются в этой области, в основном это предприятия с площадью обработки от 3000 гектаров, что указывает на необходимость повышения информированности у малых хозяйств.



Рис. 2. Осведомленность о концепции умного сельского хозяйства, %
Источник: составлено авторами по результатам исследования.

Наиболее известные технологии умного сельского хозяйства показаны на рис. 3. GPS-навигация считается универсально популярной технологией (100%), тогда как более сложные решения (IoT и облачные сервисы) знакомы менее чем трети хозяйств (27,8%). Технологии среднего уровня трудности (дроны, датчики, спутниковый мониторинг) имеют неплохую подготовленность (72-83%), что свидетельствует о постепенном внедрении инноваций в отрасль, но с явным отставанием в отрасли облачных и интернет-технологий.

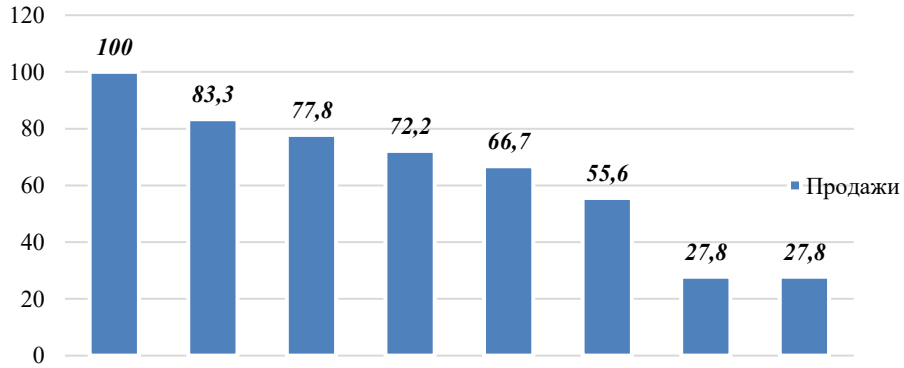

Рис. 3. Распространенность знаний о технологиях умного сельского хозяйства, %
Источник: составлено авторами по результатам исследования.

Всего 22,2% хозяйств уже активно пользуется технологиями, демонстрируя, что знание о разработках не всегда переходит в их фактическое применение (рис. 4). Однако 50% частично пользуется нововведениями, но опираясь на рис. 3 можно сказать, что это базовые технологии с низким порогом внедрения.



Рис. 4. Распределение сельскохозяйственных организаций по уровню внедрения технологий умного сельского хозяйства, %
Источник: составлено авторами по результатам исследования

Анализ навыка аграрных организаций в столкновении с киберугрозами обнаружил, что 38,9% субъектов сталкиваются с интернет-мошенничеством и попытками несанкионированного доступа (рис. 5). Это подтверждает, что организации сельского хозяйства так или иначе

соприкасаются с интернет-технологиями, что и потребовало в дальнейшем оценить восприятие ими значимости угроз информационной безопасности.

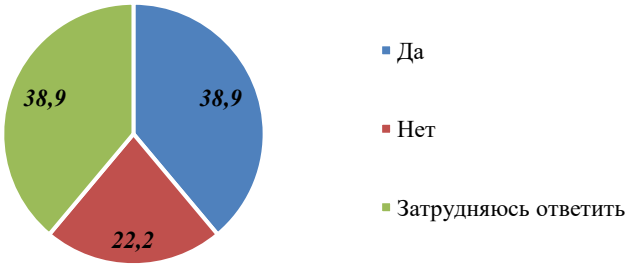

Рис. 5. Интернет-мошенничество и попытки несанкционированного доступа, %
Источник: составлено авторами по результатам исследования.

Опросы продемонстрировали высочайший уровень уязвимости аграрных организаций к мошеннической деятельности. Приблизительно 45% хозяйств уже встретились с попытками неразрешенного доступа к собственным данным и финансам. Тревожным считается и то, что 38,9% указали о практических происшествиях интернет-мошенничества. Существенная часть ответов "затруднились ответить" (38,9% и 33,3%) говорит об неудовлетворительной подготовленности руководства к происходящим конфликтам, что может указывать на неимение соответствующего мониторинга и документирования киберугроз.

Более половины хозяйств (55,6%) уже встретились с заражением компьютеров вирусами (рис. 6), что доказывает настоящее воздействие киберугроз на сельскохозяйственный сектор.



Заражение компьютеров вирусами Материальные убытки от мошенничества

Рис. Заражение компьютеров вирусами и материальные убытки, %
Источник: составлено авторами по результатам исследования.

Однако противоречиво, что 66,7% хозяйств не указали о материальных ущербах или затруднились ответить, несмотря на то, что именно сельское хозяйство наиболее быстро переводит информационный угрозы в реальные экономические потери. Это может указывать на следующие причины:

1) недостаточное понимание связи между киберинцидентами и финансовыми потерями;
2) скрытые убытки, которые не были идентифицированы как результат кибератак;
3) низкий уровень учета киберрисков в финансовом управлении.

Только 33,3% хозяйств (6 организаций) признали присутствие ущербов, что говорит об опасном пробеле в осознании финансового убытка от киберугроз в аграрном хозяйстве.

Исследование выявило высокий уровень осведомленности об определенных видах киберугроз (рис. 7). Следовательно, большинство хозяйств знакомы с обычными киберугрозами, однако меньше половины осведомлены о более специфичных для аграрного хозяйства опасностях, таких как взломы систем управления техникой и DDoS-атаки.

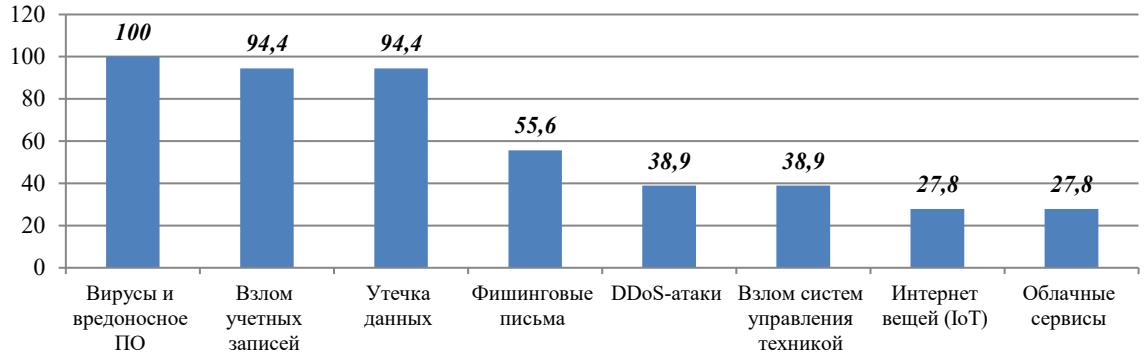

Рис. 7. Идентифицируемые типы киберугроз на предприятиях АПК, %
Источник: составлено авторами по результатам исследования.

При этом вероятность кибератаки на сельскохозяйственное предприятие оценивается как средняя 44,4% анализированными предприятиями и низкая – 22,2% (рис. 8).

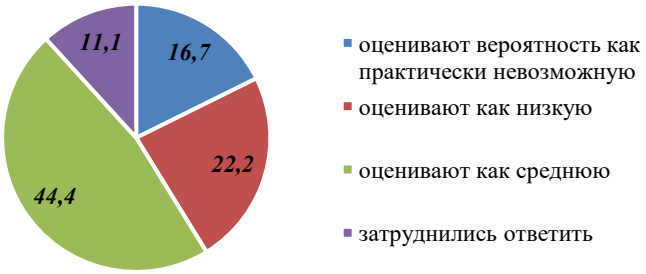

Рис. 8. Оценка вероятности кибератаки на сельскохозяйственное предприятие, %
Источник: составлено авторами по результатам исследования.

Следует отметить, что ни одно хозяйство не отметило вероятность кибератаки как существенную. Это демонстрирует недооценку риска или на то, что аграрные фирмы считают себя как менее интересные цели для киберпреступников по сравнению с серьезными корпорациями. Во многом видимо это связано с тем, что современные средства информации меньше акцентируют внимание на киберугрозы для сельского хозяйства в большей степени популяризируя угрозы для банковской сферы, энергетики и транспорта. При этом, все обследованные хозяйства допускали опасность вероятных эффектов кибератак (рис. 9), что показывает, что аграрные компании осознают существенность вероятных последствий кибератак.

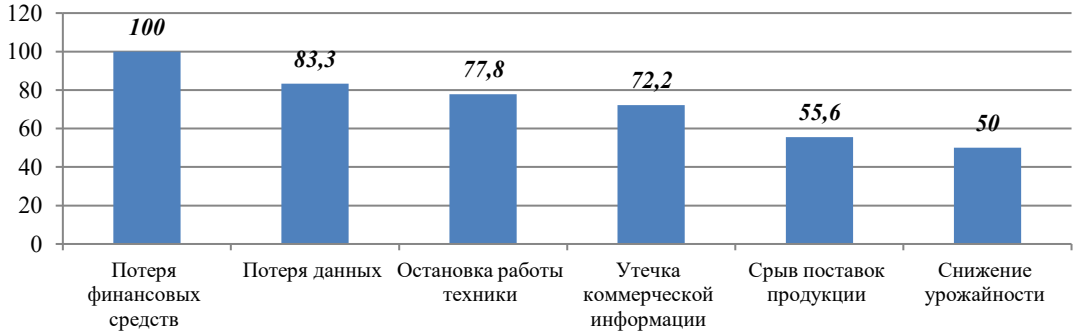

Рис. 9. Наиболее часто упоминаемые последствия, %
Источник: составлено авторами по результатам исследования.

Все опрошенные хозяйства могут использовать антивирусное программное обеспечение, однако только половина пользуется более сложными паролями, а менее тридцати процентов могут использовать вспомогательное копирование и ограниченность допуска (табл. 1). Это свидетельствует, что мероприятия охраны остаются на базовом уровне и не охватывают целостный проход к кибербезопасности. Ни одно из исследованных хозяйств не применяет двухфакторную аутентификацию, кодирование информации или системы прогноза безопасности. Это свидетельствует о том, о том, что аграрные организации используют только наиболее базовые планы защиты, которые зачастую интегрированы в операционные доктрины и обычное программное обеспечение.

Таблица 1

Применяемые меры защиты информации в сельскохозяйственных организациях

Мера защиты	Количество хозяйств	%
Антивирусное ПО	18	100
Сложные пароли	9	50
Резервное копирование данных	5	27,8
Ограничение доступа сотрудников	5	27,8
Двухфакторная аутентификация	0	0
Шифрование данных	0	0
Системы мониторинга безопасности	0	0

Источник: составлено авторами по результатам исследования.

Исследование выявило соответствующее распределение готовности хозяйств к вложениям в цифровую и кибербезопасность (рис. 10) - только 11,1% хозяйств подчистую склонны вкладывать средства в кибербезопасность, в то время как половина либо не готова, либо полагает это бесполезным.

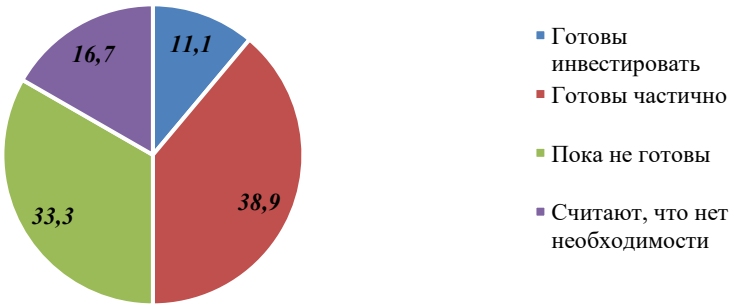

Рис. 10. Распределение сельскохозяйственных организаций по готовности инвестировать в кибербезопасность, %

Источник: составлено авторами по результатам исследования.

Основные причины, которые мешают введению технологий умного аграрного хозяйства являются показаны на рис. 11.

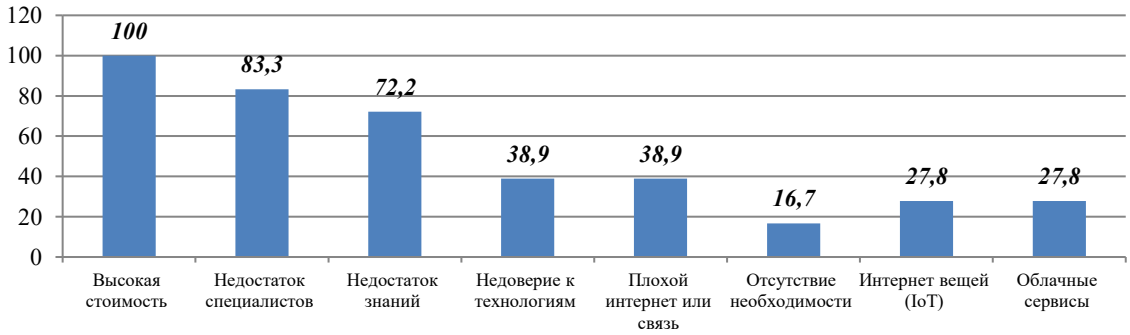

Рис. 11. Основные причины, которые препятствуют внедрению технологий умного сельского хозяйства, %

Источник: составлено авторами по результатам исследования.

Высокая себестоимость считается глобальным препятствием для всех исследованных хозяйств, что указывает на незаменимость государственной помощи и субсидирования введения технологий умного аграрного хозяйства.

Анализ выявил внутренние цифровые риски, которые аграрные организации считают наиболее потенциально опасными (табл. 2).

Таблица 2

Внутренние цифровые риски в сельскохозяйственных организациях

Тип риска	Количество хозяйств	%
Ошибки при вводе данных	13	72,2
Использование слабых паролей	13	72,2
Низкий уровень цифровых навыков	13	72,2
Потеря важных документов	12	66,7
Передача доступа посторонним лицам	11	61,1
Невнимательность при работе с письмами	10	55,6

Источник: составлено авторами по результатам исследования.

Три вида внутренних рисков (погрешности при вводе информации, применение слабых паролей и незначительный уровень цифровых способностей) в одинаковой мере многократно упоминаются как более возможные. Это показывает на то, что человеческий фактор считается решающим компонентом в системе кибербезопасности аграрных организаций.

На рис. 12 представлена информация об обучении сотрудников, из которого видно, что более 70% исследованных хозяйств не организовывают обучение, что существенно увеличивает угрозы внутренних рисков.

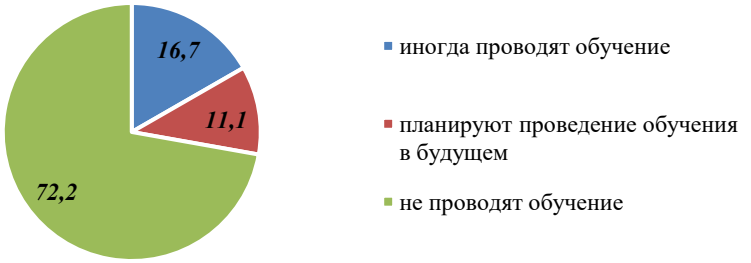

Рис. 12. Проведение обучения по кибербезопасности, %
Источник: составлено авторами по результатам исследования.

На рис. 13 показано, что в 88,9% хозяйств встречаются случаи применения личных устройств работниками для рабочих вопросов. Это формирует вспомогательный вектор для киберугроз, поскольку частные устройства зачастую имеют более низкий уровень защиты и имеют все шансы быть заражены вредоносным ПО.

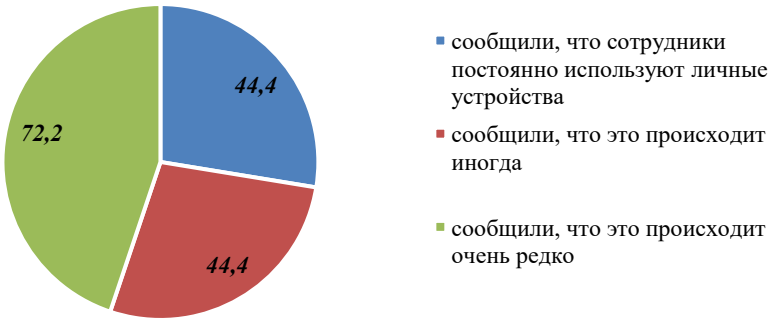

Рис. 13. Использование личных устройств для рабочих задач, %
Источник: составлено авторами по результатам исследования.

Большинство хозяйств признают существенное воздействие человеческого фактора на происхождение киберрисков (рис. 14), однако это не переходит в конструктивные меры по обучению и увеличению осведомленности работников.

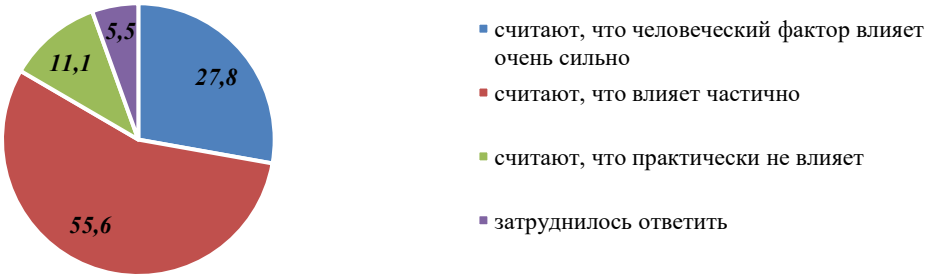

Рис. 14. Оценка влияния человеческого фактора на киберриски, %
Источник: составлено авторами по результатам исследования.

Дискуссия

Проведенное исследование обнаружило связь между уровнем цифровизации аграрных организаций и возможностью появления. Хозяйства, которые конструктивно применяют компьютеры и вводят схемы умного аграрного хозяйства, больше сталкиваются с киберугрозами. К примеру, среди хозяйств, конструктивно использующих компьютеры, 70% сообщили о заражении вирусами, потом как среди хозяйств, использующих их выборочно, этот процент составил 43%.

Однако более цифровизированные хозяйства также демонстрируют лучшую подготовленность о киберугрозах и применяют более сложные планы защиты. Хозяйства, конструктивно использующие схемы умного аграрного хозяйства, чаще употребляют сложные пароли (75% против 33% у наименее цифровизированных хозяйств) и дополнительное дублирование информации (50% против 11%). Это указывает на то, что цифровизация сама по себе не считается ключом от киберрисков, но формирует технические условия, при которых эти опасности смогут осуществляться.

Проведенное исследование доказывает, что умное аграрное хозяйство, невзирая на существенные достоинства для производительности и производительности, действительно считается источником новейших киберрисков для аграрных организаций (рис. 15).

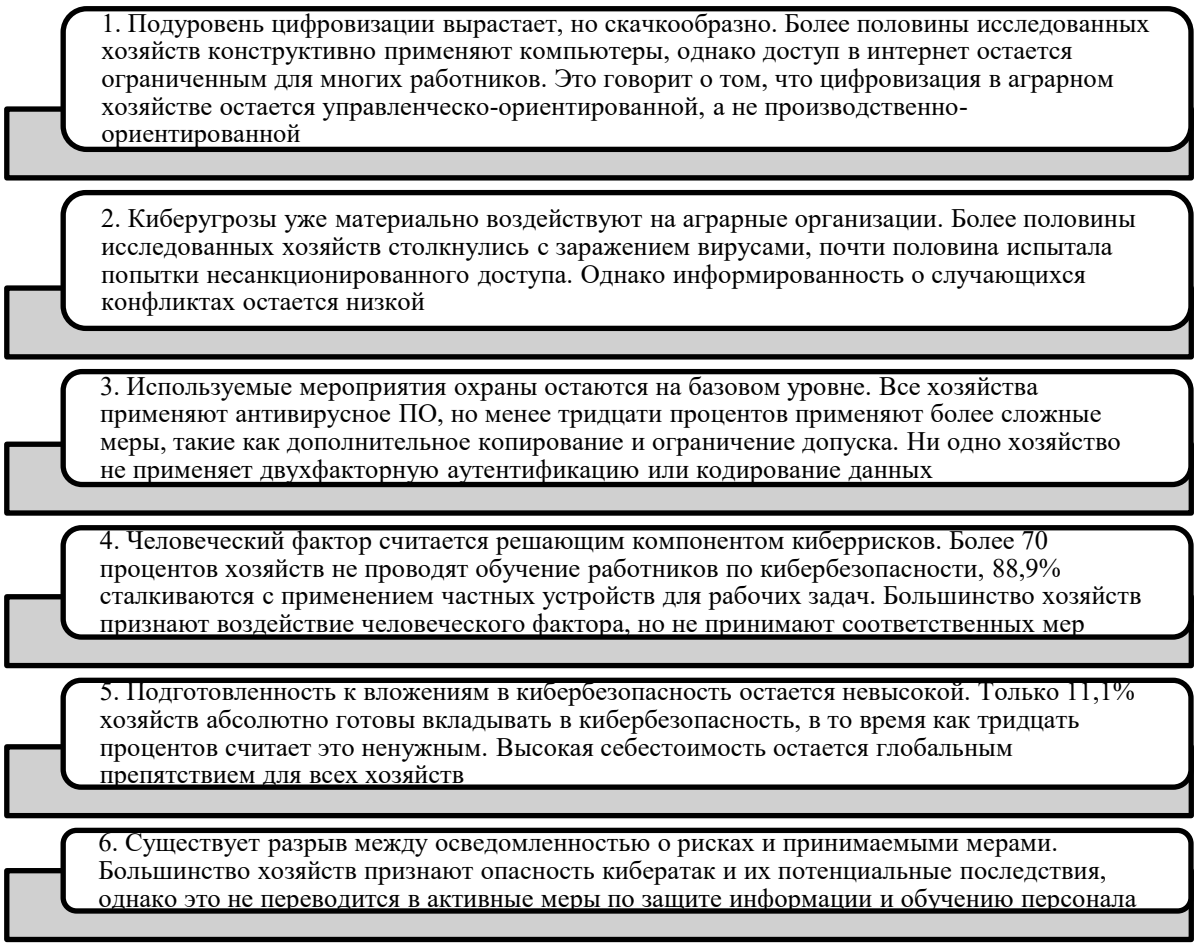

Рис. 15. Обобщенные выводы

Источник: составлено авторами по результатам исследования.

Представленный опрос позволил сформировать приоритетные меры снижения рисков:

А: Организационные меры:

• Назначить ответственных за кибербезопасность, включая производственные системы.

• Составить реестр оборудования, ПО, облачных сервисов, потоков данных и внешних подключений.

• Для каждого критичного процесса определить максимально допустимый простой и допустимую потерю данных.

• Подготовить сценарии реагирования: шифрование серверов, потеря облака, отказ связи, подозрение на подмену измерений.

• Проводить учения перед посевной, уборкой и другими критическими периодами.

• Обучать сотрудников противодействию фишингу и проверке запросов на удалённое подключение.

Для систематизации управления можно использовать NIST Cybersecurity Framework 2.0: управление, выявление, защита, обнаружение, реагирование и восстановление.

Б: Технические меры:

1. Разделение сетей.

Изолировать офисную инфраструктуру от технологических систем; разрешать только необходимые межсегментные соединения. Не размещать интерфейсы управления производственным оборудованием в открытом интернете.

2. Защита удаленного доступа.

Использовать индивидуальные учётные записи, многофакторную аутентификацию на шлюзах доступа, ограничение времени подключения и журналирование действий подрядчиков.

3. Резервное копирование и проверка восстановления.

Сохранять не только документы и базы данных, но и конфигурации контроллеров, производственные рецептуры, задания, настройки серверов и необходимые лицензии. Часть копий должна быть недоступна для изменения из основной сети.

4. Автономные и безопасные режимы.

Критические процессы не должны полностью зависеть от интернета. Необходимо предусмотреть локальное управление, безопасные состояния при отказах и отработанные ручные процедуры там, где это технологически допустимо.

5. Контроль достоверности данных.

Сопоставлять показания независимых источников, проверять физически допустимые диапазоны и выявлять необычные изменения. Для опасных операций задавать ограничения, которые нельзя обойти одной ошибочной командой аналитической системы.

6. Управление обновлениями.

Тестировать обновления до установки на производство и согласовывать обслуживание с агротехнологическим календарём. При невозможности обновления применять компенсирующие меры, прежде всего изоляцию и ограничение доступа.

7. Мониторинг.

Контролировать входы в системы, изменения конфигураций и необычные соединения. Для чувствительного ОТ-оборудования предпочтительны согласованные с производителем методы; активное сканирование без подготовки может нарушить работу.

В: Требования к поставщикам:

В закупки и договоры целесообразно включать:

• срок поддержки и порядок выпуска обновлений безопасности;
• уведомление об инцидентах и уязвимостях;
• запрет общих и неизменяемых паролей;
• контроль удаленного доступа со стороны заказчика;
• возможность экспорта данных и резервного копирования;
• описание работы оборудования без облака и интернета;
• порядок восстановления и прекращения использования сервиса.

Заключение

На основе проведенного исследования можно сформулировать следующие рекомендации (табл. 3).

Таблица 3

Рекомендации

Для сельскохозяйственных организаций	Для государственных органов	Для научного сообщества
Разработать комплексную политику информационной безопасности, включающую не только технические меры, но и организационные и процедурные элементы	Разработать программы государственной поддержки для малых и средних сельскохозяйственных предприятий, направленные на внедрение мер кибербезопасности	Провести дополнительные исследования по специфике киберугроз в сельском хозяйстве
Обеспечить регулярное обучение сотрудников вопросам кибербезопасности, особенно в области защиты от фишинга и социальной инженерии	Создать специализированные центры компетенции по кибербезопасности в сельском хозяйстве	Разработать методики оценки киберрисков для сельскохозяйственных организаций
Внедрить двухфакторную аутентификацию и шифрование для критически важных данных	Разработать стандарты и рекомендации по кибербезопасности, специфичные для сельскохозяйственного сектора	Создать открытые базы данных об инцидентах в сельском хозяйстве для анализа и прогнозирования угроз
Установить четкие процедуры управления доступом и использования личных устройств	Обеспечить подготовку специалистов по информационной безопасности для сельского хозяйства	
Проводить регулярные аудиты информационной безопасности и тестирование на уязвимости		

Источник: составлено авторами по результатам исследования.

Не подлежит сомнению, что умное сельское хозяйство бесспорно формирует ранее не известные киберриски, которые требуют большего внимания. Успешная цифровизация аграрного сектора вероятна только при обстоятельстве одновременного становления концепции кибербезопасности, включающей промышленные, координационные и профессиональных компоненты.

Приоритет следует отдавать не количеству установленных средств защиты, а способности предприятия:

• продолжать критические операции при инциденте;

• обнаруживать недостоверные данные;

• безопасно управлять оборудованием;

• восстанавливаться за время, приемлемое для конкретного агротехнологического процесса.

Литература

1. Об утверждении стратегического направления в области цифровой трансформации отраслей агропромышленного и рыбохозяйственного комплексов РФ на период до 2030 г., распоряжение Правительства РФ от 29 декабря 2021 г. № 3971-р.

2. Батистова О.И. Смарт-фермерство в России: современное состояние и стратегические вызовы // Международный сельскохозяйственный журнал. 2025. № 6. С. 767-772. DOI 10.55186/25876740_2025_68_6_767.

3. Белоусов С.А., Фролова О.А., Лайша А.К. Цифровые подходы к повышению производительности труда в агропромышленном комплексе // Вестник евразийской науки. 2025. Т. 17. № 3. С. 5.

4. Глазьев С.Ю., Сухарев О.С. Производительность труда: измерение и возможности повышения // Journal of new economy. 2026. Т. 27. № 1. С. 6-27. DOI 10.29141/2658-5081-2026-27-1-1.

5. Гришунин С.В., Пищалкина И.Ю., Сулоева С.Б. Оценка киберрисков в проектах интернета вещей // π-Economy. 2021. Т. 14. № 6. С. 102-116. DOI 10.18721/JE.14608.

6. Киленников А.Я. Исследование потребности в навыках использования искусственного интеллекта персоналом агропредприятий / Искусственный интеллект в принятии экономических решений: активы, акторы, стратегии: монография (серия «Управление активами») / под ред. И.М. Степнова, Ю.А. Ковальчук; МГИМО МИД России. Москва: ЦЭМИ РАН, 2026. 950 с. С. 781-787.

7. Косников С.Н. и др. Производительность труда в сельском хозяйстве в условиях цифровизации и развития человеческого капитала // Фундаментальные исследования. 2026. № 5. С. 128-133. DOI 10.17513/fr.44031.

8. Магомедов А.М. От информатизации к цифровизации сельского хозяйства: методологические подходы // УЭПС: управление, экономика, политика, социология. 2023. № 2. С. 59-64. DOI 10.24412/2412-2025-2023-2-59-64.

9. Назаров Д.М. и др. Кибербезопасность в агропромышленном комплексе России: инструменты, кейсы, инциденты // Международный сельскохозяйственный журнал. 2026. № 3. С. 417-420. DOI 10.55186/25876740_2026_69_3_417.

10. Пчелинцева Н.В., Воропаев Д.И. Влияние цифровизации на устойчивое развитие сельского хозяйства // Наука и Образование. 2026. Т. 9. № 1. С. 110.

11. Продовольственная и сельскохозяйственная организация Объединенных Наций. Умное сельское хозяйство. URL: https://www.fao.org/smart-farming/ru.

12. CAO B. et al. Current status, challenges and prospects of smart agriculture technology development in China // Transactions of the Chinese Society of Agricultural Engineering. 2025. Vol. 41. No. 21. P. 1-10. DOI 10.11975/j.issn.1002-6819.202505242.

13. Ke X. et al. Research on the impact of digital-intelligence integration on agricultural industry resilience: evidence from China // Frontiers in Sustainable Food Systems. 2025. Vol. 9. P. 1677559. DOI 10.3389/fsufs.2025.1677559.

References

1. On approval of the strategic direction in the field of digital transformation of the agro-industrial and fisheries sectors of the Russian Federation for the period up to 2030, Decree of the Government of the Russian Federation dated December 29, 2021 No. 3971-R. (In Russian)
2. Batistova O.I. Smart farming in Russia: current state and strategic challenges // International Agricultural Journal. 2025. No. 6. P. 767-772. DOI 10.55186/25876740_2025_68_6_767. (In Russian)
3. Belousov S.A., Frolova O.A., Laisha A.K. Digital approaches to increasing labor productivity in the agro-industrial complex // Bulletin of Eurasian Science. 2025. Vol. 17. No. 3. P. 5. (In Russian)
4. Glazyev S.Yu., Sukharev O.S. Labor productivity: measurement and opportunities for improvement // Journal of new economy. 2026. Vol. 27. No. 1. P. 6-27. DOI 10.29141/2658-5081-2026-27-1-1. (In Russian)
5. Grishunin S.V., Pishchalkina I.Yu., Suloeva S.B. Assessment of cyber risks in Internet of Things projects // pi-Economy. 2021. Vol. 14. No. 6. P. 102-116. DOI 10.18721/JE.14608. (In Russian)
6. Kilennikov A.Ya. Research of the need for skills in using artificial intelligence by personnel of agricultural enterprises / Artificial intelligence in making economic decisions: assets, actors, strategies: monograph (series "Asset Management") / edited by I.M. Stepnov, Yu.A. Kovalchuk; MGIMO Ministry of Foreign Affairs of Russia. Moscow: CEMI RAS, 2026. 950 p. P. 781-787. (In Russian)
7. Kosnikov S.N. et al. Labor productivity in agriculture in the context of digitalization and human capital development // Fundamental Research. 2026. No. 5. P. 128-133. DOI 10.17513/fr.44031. (In Russian)
8. Magomedov A.M. From informatization to digitalization of agriculture: methodological approaches // UES: management, economics, politics, sociology. 2023. No. 2. P. 59-64. DOI 10.24412/2412-2025-2023-2-59-64. (In Russian)
9. Nazarov D.M. et al. Cybersecurity in the Russian agro-industrial complex: tools, cases, incidents // International Agricultural Journal. 2026. No. 3. P. 417-420. DOI 10.55186/25876740_2026_69_3_417. (In Russian)
10. Pchelintseva N.V., Voropaev D.I. The impact of digitalization on the sustainable development of agriculture // Science and Education. 2026. Vol. 9. No. 1. P. 110. (In Russian)
11. Food and Agriculture Organization (FAO). Smart Farming. URL: https://www.fao.org/smart-farming/ru. (In Russian)
12. CAO B. et al. Current status, challenges and prospects of smart agriculture technology development in China // Transactions of the Chinese Society of Agricultural Engineering. 2025. Vol. 41. No. 21. P. 1-10. DOI 10.11975/j.issn.1002-6819.202505242.
13. Ke X. et al. Research on the impact of digital-intelligence integration on agricultural industry resilience: evidence from China // Frontiers in Sustainable Food Systems. 2025. Vol. 9. P. 1677559. DOI 10.3389/fsufs.2025.1677559.

Об авторах

Иванова Анастасия Алексеевна, студент, Финансовый университет при Правительстве РФ, Москва.

Киленников Александр Янович, студент, Финансовый университет при Правительстве РФ, Москва.

Степнов Игорь Михайлович, доктор экономических наук, профессор, профессор кафедры корпоративных финансов и корпоративного управления, Финансовый университет при Правительстве РФ, Москва.

About authors

Anastasia A. Ivanova, student, Financial University under the Government of the Russian Federation, Moscow.

Aleksandr Ya. Kilennikov, student, Financial University under the Government of the Russian Federation, Moscow.

Igor M. Stepnov, Doctor of Sci. (Econ.), Professor, Leading Researcher at the Market Economy Institute of the Russian Academy of Sciences, Moscow; Professor of Department of Corporate Finance and Corporate Governance of Financial University under the Government of the Russian Federation, Moscow.