

Научно-исследовательский
центр «Иннова»

**ФУНДАМЕНТАЛЬНАЯ И ПРИКЛАДНАЯ
НАУКА: НАУЧНО-МЕТОДИЧЕСКИЕ
И ПРАКТИЧЕСКИЕ АСПЕКТЫ**

Сборник научных трудов по материалам
XI Международной научно-практической конференции,
20 апреля 2026 года, г.-к. Анапа



Анапа
2026

УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5
Ф94

Главный редактор:
Скорикова Екатерина Николаевна

Редакционная коллегия:

Бондаренко С. В., к.э.н., профессор (Россия, г. Краснодар), **Дегтярев Г. В.**, д.т.н., профессор (Россия, г. Краснодар), **Хилько Н. А.**, д.э.н., доцент (Россия, г. Анапа), **Ожерельева Н. Р.**, к.э.н., доцент (Россия, г. Анапа), **Жиянова Н. Э.**, к.э.н., профессор (Узбекистан, г. Ташкент), **Климов С. В.** к.п.н., доцент (Россия, г. Пермь), **Михайлов В. И.** к.ю.н., доцент (Россия, г. Москва).

Ф94 **Фундаментальная и прикладная наука: научно-методические и практические аспекты.** Сборник научных трудов по материалам XI Международной научно-практической конференции (г.-к. Анапа, 20 апреля 2026 г.). – Анапа: НИЦ ЭСП в ЮФО, 2026. – 68 с.

ISBN 978-5-95356-989-7

В настоящем издании представлены материалы XI Международной научно-практической конференции «Фундаментальная и прикладная наука: научно-методические и практические аспекты», состоявшейся 20 апреля 2026 года в г.-к. Анапа. Материалы конференции посвящены актуальным проблемам науки, общества и образования. Рассматриваются теоретические и методологические вопросы в социальных, гуманитарных, естественных и других науках.

Издание предназначено для научных работников, преподавателей, аспирантов, всех, кто интересуется достижениями современной науки.

За содержание и достоверность статей, а также за соблюдение законов об интеллектуальной собственности ответственность несут авторы. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

Информация об опубликованных статьях размещена на платформе научной электронной библиотеки (eLIBRARY.ru). **Договор № 2341-12/2017К от 27.12.2017 г.**

Электронная версия сборника находится в свободном доступе на сайте:
www.innova-science.ru.

УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5

ISBN 978-5-95356-989-7

© Коллектив авторов, 2026.
© ООО «НИЦ ЭСП» в ЮФО
(подразделение НИЦ «Иннова»), 2026.

СОДЕРЖАНИЕ

БИОЛОГИЧЕСКИЕ НАУКИ

ОБЗОР БИОЛОГИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ РАСТЕНИЙ ОТ ФИТОПАТОГЕНОВ

Газизова Гульнур Ришатовна 5

ФАРМАЦЕВТИЧЕСКИЕ НАУКИ

О НОРМАТИВНЫХ ТРЕБОВАНИЯХ К ПОМЕЩЕНИЯМ ПРОИЗВОДСТВЕННЫХ АПТЕК В СТРАНАХ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

*Дударенкова Марина Рудольфовна, Солонина Анна Владимировна
Горбунова Екатерина Сергеевна* 11

ТЕХНИЧЕСКИЕ НАУКИ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ТРАНСФОРМАЦИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ: ОТ АВТОМАТИЗАЦИИ К ПЕРЕОПРЕДЕЛЕНИЮ ЗАНЯТОСТИ

*Зиганшин Шамиль Эльмирович
Габдлхакова Лиана Фидановна* 20

УЯЗВИМОСТИ СИСТЕМ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ: АТАКИ НА ОБУЧЕНИЕ И ВНЕДРЕНИЕ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ

*Ивинских Игорь Валерьевич
Кияшко Милана Антоновна* 25

РАЗРАБОТКА МОДЕЛЕЙ ДИЗЕЛЬНОГО ТОПЛИВА ДЛЯ ОЦЕНКИ СТАБИЛЬНОСТИ ЕГО СВОЙСТВ ПРИ ХРАНЕНИИ С МОРСКОЙ ВОДОЙ

Нелюбов Дмитрий Владимирович 38

ЭКОНОМИЧЕСКИЕ НАУКИ

AGILE-МЕТОДОЛОГИИ В РОССИЙСКИХ СТАРТАПАХ: ЭКОНОМИЧЕСКИЕ ФАКТОРЫ ВЫБОРА И РЕЗУЛЬТАТИВНОСТИ

Канзепаров Руслан Ринатович..... 44

**ЗАРУБЕЖНЫЙ ОПЫТ АГРАРНОЙ ПОЛИТИКИ В УСЛОВИЯХ
ЦИФРОВИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА**

Самыкин Иван Витальевич 50

ЮРИДИЧЕСКИЕ НАУКИ

**НОВЫЕ ПОДХОДЫ К ОХРАНЕ НЕДВИЖИМОГО ИМУЩЕСТВА
В УСЛОВИЯХ РОСТА КИБЕРМОШЕННИЧЕСТВА И РЕЙДЕРСТВА
В РОССИИ**

Малыгина Ия Максимовна..... 60

БИОЛОГИЧЕСКИЕ НАУКИ

УДК 632.937

ОБЗОР БИОЛОГИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ РАСТЕНИЙ ОТ ФИТОПАТОГЕНОВ

Газизова Гульнур Ришатовна

магистрант

ФГАОУ ВО НИУ ИТМО,

ГАОУ ВО АГТУ «Высшая школа нефти»,

город Альметьевск

***Аннотация.** В статье рассмотрены биологические средства защиты растений от фитопатогенов, применяемые в современной агробиологии. Охарактеризованы основные группы антагонистических микроорганизмов, включая бактерии родов *Bacillus* и *Pseudomonas*, а также грибы рода *Trichoderma*. Показаны механизмы подавления возбудителей болезней, среди которых конкуренция за питательный субстрат, антибиоз, микопаразитизм, ферментативный лизис и индукция устойчивости растений. На основе публикаций российских авторов обобщены сведения о результативности биопрепаратов против корневых гнилей, пятнистостей, фитофтороза и других инфекций.*

*The article discusses biological plant protection products against phytopathogens used in modern agrobiolgy. The main groups of antagonistic microorganisms, including bacteria of the genera *Bacillus* and *Pseudomonas*, as well as fungi of the genus *Trichoderma*, are characterized. The mechanisms of suppression of pathogens are shown, including competition for a nutrient substrate, antibiosis, mycoparasitism, enzymatic lysis, and induction of plant resistance. Based on the publications of Russian authors, information on the effectiveness of biologics against root rot, blotches, late blight and other infections is summarized.*

Ключевые слова: биозащита, фитопатогены, биопрепараты,

антагонисты, ризосфера

Key words: *biosecurity, phytopathogens, biologics, antagonists, rhizosphere*

Фитопатогенные грибы, бактерии и оомицеты формируют устойчивый инфекционный фон в посевах, теплицах и хранилищах. Потери урожая складываются не только из прямого угнетения роста, но и из ухудшения посевных качеств, падения товарности, накопления токсичных метаболитов, сокращения сроков хранения. На фоне длительного использования химических фунгицидов в агроценозах нарастает селекционное давление на популяции возбудителей, меняется их чувствительность, нарушается микробное равновесие ризосферы. По данной причине интерес к биологическим средствам защиты устойчиво растет. Научное сообщество рассматривает биоконтроль болезней растений не в роли вспомогательного приема, а в составе самостоятельного направления, объединяющего микробиологию, фитопатологию, биотехнологию и агроэкологию [3, с. 421].

Российские исследования показывают, что биологическая защита от фитопатогенов опирается на несколько групп агентов. Первая группа включает антагонистические грибы. В учебнике М. В. Штерншис, И. В. Андреевой и О. Г. Томиловой указано, что виды рода *Trichoderma* подавляют *Fusarium*, *Pythium*, *Phoma*, *Phytophthora*, *Alternaria*, *Botrytis* и ряд иных возбудителей за счет микопаразитизма, антибиоза и конкурентного вытеснения, а отдельные формы дополнительно запускают болезнеустойчивость растения и стимулируют рост [5, с. 214]. Вторая группа объединяет спорообразующие бактерии рода *Bacillus*. Их практическая ценность определяется устойчивостью к неблагоприятным условиям, хорошей технологичностью и широким спектром антимикробного действия. Третья группа представлена псевдомонадами, актиномицетами, дрожжами и смешанными композициями, способными колонизировать ризосферу, филлосферу либо раневые поверхности плодов.

С позиций механизма действия отечественные авторы выделяют несколько линий подавления патогена. Среди них конкуренция за субстрат и место обитания, синтез антибиотических соединений, секреция гидролитических ферментов, разрушение клеточной стенки возбудителя, образование биопленки на

корневой поверхности, индукция системной устойчивости. По данным Т. М. Сидоровой, А. М. Асатуровой и А. И. Хомяк, *Bacillus subtilis* продуцирует липопептиды, полипептиды, белки и иные вторичные метаболиты, причем часть соединений не только угнетает фитопатогены, но и работает в роли элиситоров защитных реакций растения [4, с. 29–30]. Подобный набор механизмов делает бактериальные препараты пригодными для профилактики корневых гнилей, пятнистостей, фитофтороза, альтернариоза, мучнисторосяных инфекций.

Отдельное место занимают препаративные формы, где микроб сочетается с веществом, усиливающим ответ растения. В полевых опытах И. И. Новиковой с соавторами комплексы на основе штаммов *Bacillus subtilis* и хитозана снижали пораженность яровой пшеницы комплексом болезней на 17,9 %, а по общей результативности превосходили отдельные биопрепараты на 16,2 % [2, с. 158]. Полученные данные подтверждают продуктивность комбинированного подхода, при котором прямое антагонистическое действие соединяется с запуском иммунных и физиологических реакций культуры.

Современный рынок биологических средств защиты от фитопатогенов условно делится на четыре функциональные группы. Первая включает монокомпонентные бактериальные препараты на основе *Bacillus subtilis* и близких видов. В российской практике к данной группе относятся формы, применяемые при обработке семян, клубней, посадочного материала и вегетирующих растений. Вторая группа объединяет грибные препараты на основе *Trichoderma* spp. Третья группа включает бактериальные препараты на основе *Pseudomonas fluorescens* и иных ризосферных антагонистов. Четвертая группа формируется из полифункциональных композиций, куда входят микробные клетки, метаболиты, элиситоры, прилипатели, носители и стабилизаторы. Учебник по биологической защите растений фиксирует присутствие в российском ассортименте препаратов Бактофит, Фитоспорин-М, Алирин-Б, Гамаир, Витаплан и Ризоплан, применяемых против корневых гнилей, фитофтороза, ризоктониоза, альтернариоза, мучнистой росы и иных инфекций [5, с. 229].

Сильная сторона биологических средств состоит в полимеханистическом

действию. В отличие от одноцелевого химического фунгицида, микробный препарат способен одновременно ограничивать прорастание спор, замедлять рост мицелия, перестраивать микробный ценоз ризосферы, усиливать рост корней и повышать устойчивость растения к повторному заражению. Подобная многослойность повышает стабильность защитного эффекта в неоднородной полевой среде. Однако универсального решения для всех патосистем пока нет. Результат зависит от штамма, препаративной формы, фазы развития культуры, влажности, температуры, степени инфекционного фона, совместимости с агроприемами и химическими препаратами.

Перспективным направлением служит подбор штаммов под конкретный патоккомплекс. Работы с бактериями-антагонистами против желтой пятнистости пшеницы показали заметную вариабельность действия даже внутри одного рода. В опытах О. Ю. Кремневой, А. М. Асатуровой, М. Д. Жарниковой и Г. В. Волковой штамм *Bacillus* sp. BZR 18 подавлял развитие болезни в диапазоне 68,5–83,0 %, при этом иные бактериальные культуры действовали слабее [1, с. 99]. Следовательно, эффективность определяется не только родовой принадлежностью агента, но и индивидуальными физиолого-биохимическими свойствами продуцента. Для практики отсюда вытекает необходимость скрининга, оценки стабильности признаков, проверки технологичности культивирования и контроля жизнеспособности при хранении.

Большой интерес вызывают метаболитные и комбинированные продукты. Живая культура способна работать дольше, но чувствительна к условиям среды и качеству формуляции. Комплекс метаболитов действует быстрее, зато срок защитного эффекта нередко короче. Комбинация живых клеток с метаболитами, хитозаном, гуминовыми веществами или микроэлементами открывает путь к усилению действия без чрезмерного увеличения дозы. Для селекции штаммов приоритет получают продуценты с выраженной способностью к колонизации корня, синтезу липопептидов, ферментов литического комплекса, сидерофоров и сигнальных молекул, запускающих устойчивость хозяина.

Практический вывод для агрономической службы состоит в переходе от

схемы разовой обработки к системе сопровождения культуры. Биопрепарат показывает лучший результат при раннем внесении, профилактическом режиме и повторном применении в уязвимые фазы. Высокий эффект достигается при сочетании обработки семян с последующим опрыскиванием вегетирующих растений, при использовании устойчивых сортов, соблюдении севооборота, оптимизации питания и снижении травмирования тканей. Биологическое средство в подобных схемах выступает не изолированным продуктом, а частью управляемого фитосанитарного контура.

Биологические средства защиты растений от фитопатогенов представляют зрелое направление современной агробиологии. Российские исследования убедительно показывают результативность препаратов на основе *Trichoderma*, *Bacillus*, *Pseudomonas* и полифункциональных композиций.

Максимальный производственный эффект достигается при включении биосредств в интегрированную систему защиты культуры, где учитываются сроки внесения, инфекционный фон, состояние почвы и биология возбудителя.

Список литературы

1. Кремнева, О. Ю. Штаммы бактерий — антагонистов *Rhizoglyphus tritici-repentis* in vitro, эффективные против желтой пятнистости листьев пшеницы в фазу всходов в вегетационном опыте / О. Ю. Кремнева, А. М. Асатурова, М. Д. Жарникова, Г. В. Волкова / Сельскохозяйственная биология. — 2015. — Т. 50, № 1. — С. 99–106. — DOI 10.15389/agrobiology.2015.1.99rus.

2. Новикова, И. И. Устойчивость к болезням, продуктивность и содержание фотосинтетических пигментов в листьях яровой мягкой пшеницы (*Triticum aestivum* L.) под влиянием полифункциональных биопрепаратов и комплексов на основе микроорганизмов и хитозана / И. И. Новикова, Э. В. Попова, Л. Е. Колесников, Ю. Р. Колесникова, С. С. Чекурова / Сельскохозяйственная биология. — 2023. — Т. 58, № 1. — С. 158–183. — DOI 10.15389/agrobiology. 2023. 1. 158rus.

3. Павлюшин, В. А. Микробиологическая защита растений в технологиях фитосанитарной оптимизации агроэкосистем. Теория и практика. Обзор / В. А.

Павлюшин, И. И. Новикова, И. В. Бойкова / Сельскохозяйственная биология. — 2020. — Т. 55, № 3. — С. 421–438. — DOI 10.15389/agrobiology.2020.3.421rus.

4. Сидорова, Т. М. Биологически активные метаболиты *Bacillus subtilis* и их роль в контроле фитопатогенных микроорганизмов. Обзор / Т. М. Сидорова, А. М. Асатулова, А. И. Хомяк / Сельскохозяйственная биология. — 2018. — Т. 53, № 1. — С. 29–37. — DOI 10.15389/agrobiology.2018.1.29rus.

5. Штерншис, М. В. Биологическая защита растений: учебник для вузов / М. В. Штерншис, И. В. Андреева, О. Г. Томилова. — 6-е изд., стер. — Санкт-Петербург: Лань, 2022. — 332 с. — ISBN 978-5-8114-9501-6.

ФАРМАЦЕВТИЧЕСКИЕ НАУКИ

УДК 615.12

О НОРМАТИВНЫХ ТРЕБОВАНИЯХ К ПОМЕЩЕНИЯМ ПРОИЗВОДСТВЕННЫХ АПТЕК В СТРАНАХ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

Дударенкова Марина Рудольфовна

к.фарм.н., доцент

ФГБОУ ВО «Оренбургский государственный медицинский университет»

Минздрава России, город Оренбург

Солонина Анна Владимировна

д.фарм.н., профессор

ФГБОУ ВО «Пермская государственная фармацевтическая академия»

Минздрава Росси, город Пермь

Горбунова Екатерина Сергеевна

старший преподаватель кафедры управления и экономики фармации,

фармацевтической технологии и фармакогнозии

ФГБОУ ВО «Оренбургский государственный медицинский университет»

Минздрава России, город Оренбург

***Аннотация.** В статье проведен анализ нормативных документов, регламентирующих обращение лекарственных средств, правила надлежащей аптечной практики, виды аптечных организаций, осуществляющих изготовление лекарственных препаратов, и требования к их помещениям в странах Евразийского экономического союза (ЕАЭС). Анализ законодательных актов, регулирующих обращение лекарственных средств, свидетельствует о наличии производственных аптек и их необходимости во всех странах ЕАЭС, отдельно в видах аптек предусмотрены аптеки медицинских организаций. Во всех государствах, кроме Республики Армения, утверждены требования надлежащей аптечной*

практики, разнообразные по структуре. В республике Беларусь регламентирован комплекс помещений производственных аптек, ограничения по расстоянию между аптеками и количеству аптек в одном капитальном строении. Площади помещений аптечных организаций в других странах ЕАЭС в настоящее время не нормированы.

The article analyzes the regulatory documents governing the circulation of medicines, the rules of good pharmacy practice, the types of pharmacy organizations engaged in the compounding of drugs, and the requirements for their premises in the countries of the Eurasian Economic Union (EEU). The analysis of the legislative acts regulating the circulation of medicines indicates the presence of compounding pharmacies and their necessity in all EEU countries, with separate provisions for pharmacies of medical organizations. In all countries except the Republic of Armenia, the requirements of good pharmacy practice have been approved, with varying structures. In the Republic of Belarus, the complex of premises of compounding pharmacies, restrictions on the distance between pharmacies and the number of pharmacies in one capital building are regulated. The areas of premises of pharmacy organizations in other EEU countries are currently not regulated.

Ключевые слова: обращение лекарственных средств, надлежащая аптечная практика, виды аптек, аптеки, производственные аптеки, изготовление лекарственных препаратов, помещения аптек

Keywords: circulation of medicines, good pharmacy practice, types of pharmacies, pharmacies, compounding pharmacies, compounding drugs, premises of pharmacies

Несмотря на незначительный объем реализации экстенпоральных лекарственных препаратов (ЛП) в общем товарообороте аптек [1, с. 39], различные направления исследований, связанные с деятельностью производственных аптек (ПА), остаются актуальными. В то же время, нормативные документы, рекомендации, устанавливающие требования к составу помещений ПА, в большинстве своем утратили силу [2, с. 396]. Представляют интерес подходы, применяемые на постсоветском пространстве, поскольку ряд стран входят в ЕАЭС на условиях

экономической интеграции. Проведенные ранее исследования относительно классификационных характеристик и помещений аптечных организаций в странах ЕАЭС в большей степени касались аптек готовых форм и выполнения ими отдельных функций [3, с. 43].

Целью исследования являлось проведение анализа требований к помещениям ПА в странах ЕАЭС. Задачи исследования: анализ нормативных документов, регламентирующих обращение лекарственных средств, правила надлежащей аптечной практики, виды аптечных организаций, осуществляющих изготовление экстенпоральных ЛП, и требования к их помещениям в странах ЕАЭС.

Методологическая основа исследования: теоретические труды отечественных и зарубежных ученых. Объекты исследования: законодательные нормативные акты, регламентирующие обращение лекарственных средств, и нормативные правовые акты, регламентирующие правила надлежащей аптечной практики (НАП), в странах ЕАЭС. Методы исследования: документальный анализ, систематизация, обобщение, группировка и сравнение, контент-анализ.

Требования к обращению лекарственных средств в государствах ЕАЭС регламентированы различными законодательными актами: Федеральным законом «Об обращении лекарственных средств» (Россия) [4], Законом Республики Беларусь «Об обращении лекарственных средств» [5], Кодексом Республики Казахстан «О здоровье народа и системе здравоохранения» [6], Законом Кыргызской республики «Об обращении лекарственных средств» [7], Законом Республики Армения «О лекарствах» [8].

НАП регламентирована нормативными правовыми актами разного уровня. Так, в России утверждены Правила НАП приказом Минздрава России [9], в Беларуси НАП утверждена Постановлением Министерства Здравоохранения Республики [10], в Казахстане – Приказом и.о. Министра здравоохранения Республики [11]. Правила НАП утверждены документами в сфере здравоохранения (Россия, Беларусь, Казахстан). В Республике Кыргызстан, в отличие от других фармацевтических практик, утверждаемых согласно требованиям международных договоров, НАП утверждена Кабинетом Министров [12]. В Республике

Армения термин «НАП» не предусмотрен Законом «О лекарствах», и отсутствуют соответствующие отраслевые документы.

Виды аптек, осуществляющих изготовление ЛП, в странах ЕАЭС приведены в таблице 1.

Таблица 1 – Виды аптек, осуществляющих изготовление ЛП, в странах ЕАЭС

Страны ЕАЭС	Виды аптек	Нормативное обоснование
Российская Федерация	<p>Аптека, осуществляющая розничную торговлю (отпуск) ЛП населению:</p> <ul style="list-style-type: none"> – аптека производственная с правом изготовления ЛП; – аптека производственная с правом изготовления асептических ЛП. <p>Аптека как структурное подразделение медицинской организации:</p> <ul style="list-style-type: none"> – аптека производственная с правом изготовления ЛП; – аптека производственная с правом изготовления асептических ЛП; – аптека производственная с правом изготовления радиофармацевтических ЛП. 	[13]
Республика Беларусь	<p>Аптека первой категории. Больничная аптека первой категории.</p>	[10]
Республика Казахстан	<p>Аптека с правом изготовления лекарственных форм по рецептам врачей, по требованиям или заявкам медицинских организаций, организаций просвещения и социального обеспечения, стандартным прописям, внутриаптечной заготовки в соответствии с утвержденными прописями, фасовки лекарственных средств и лекарственного растительного сырья, с приобретением лекарственных субстанций, хранением, контролем качества, оформлением и реализацией изготовленных лекарственных препаратов, в том числе гомеопатических препаратов, медицинских изделий, других товаров аптечного ассортимента населению и не относящихся к лекарственным средствам, медицинским изделиям в соответствии с перечнем, утверждаемым уполномоченным органом.</p> <p>Аптека медицинской организации (больничная, межбольничная) с правом изготовления ЛП и обеспечения лекарственными средствами.</p>	[11]
Кыргызская Республика	<p>Аптека с правом:</p> <ul style="list-style-type: none"> – изготовления лекарственных средств и препаратов по рецептам врачей по требованиям или заявкам организаций здравоохранения, стандартным прописям; – внутриаптечной заготовки лекарственных средств и препаратов в соответствии с утвержденными прописями; – фасовки лекарственных средств и препаратов, а также осуществляющие реализацию готовых лекарственных средств и 	[12]

	препаратов. Внутрибольничная аптека с правом изготовления и отпуска лекарственных средств и препаратов для обеспечения пациентов лекарственными средствами и препаратами.	
Республика Армения	Аптека*. Аптека медицинского учреждения*.	[8]
Примечание*: только аптеки, в лицензии которых имеется отметка об изготовлении ЛП.		

В числе первых государств на постсоветском пространстве, где разрабатывалась НАП в рамках международной системы менеджмента качества ISO, можно отметить Беларусь и Казахстан. В декабре 2006 года постановлением Министерства Здравоохранения Республики Беларусь была утверждена НАП [10], требования которой носили обязательный характер. В Казахстане НАП применялась субъектами обращения лекарственных средств на добровольной основе с 2006 года, а необходимость соблюдения стандарта НАП (GPP) стало обязательным только с 1 января 2018 года [14].

Российская Федерация. Российские правила НАП, в основном, ориентированы на розничную торговлю ЛП, в части изготовления «ex tempore» актуальными являются правила изготовления и отпуска ЛП [4, 9, 15], отдельным приказом установлены виды аптечных организаций [13], в числе которых аптеки производственные. В настоящее время в России определены для помещений ПА общие требования (Государственная фармакопея XV издания, ОФС.1.8.0001, ОФС.1.8.0006) и санитарно-эпидемиологические требования [16, 17], но площади помещений не нормированы.

Республика Беларусь. В законе «Об обращении лекарственных средств» НАП обозначена в числе надлежащих фармацевтических практик в сфере обращения лекарственных средств и включает совокупность правил, в т.ч. предписывающих требования к помещениям, оборудованию и классификации аптек по категориям [5]. В соответствии с НАП аптеки подразделяются на 5 категорий, больничные аптеки – на 2 категории. Производственные аптеки (аптеки и больничные аптеки), отнесены к аптекам первой категории. Для аптек первой категории обозначены функции и комплекс помещений без указания их площадей, но нормируется минимальная общая площадь ПА – не мене 100 квадратных метров. С

1 марта 2023 года вступили в силу изменения к НАП, регламентирующие размещение помещений аптек, ограничения по расстоянию между аптеками (не менее 500 метров) и количеству аптек в одном капитальном строении (одна аптека) и торговом центре (от одной до трех аптек в зависимости от площади торгового центра) [10]. Установлены специфические санитарно-эпидемиологические требования к содержанию и эксплуатации организаций здравоохранения, в т.ч. аптек [18].

Республика Казахстан. Фармацевтическая деятельность, обращение лекарственных средств медицинских изделий введены в отдельный раздел Кодекса Республики Казахстан «О здоровье народа и системе здравоохранения» [6]. Кодексом регламентирована деятельность инспектората по надлежащим фармацевтическим практикам, утвержденным единым приказом в сфере здравоохранения. Отдельная глава НАП устанавливает требования к помещениям аптечных организаций, подразделяя их на виды, одним из которых является аптека с правом изготовления лекарственных форм. В НАП регламентирован перечень отделов аптеки с правом изготовления ЛП [11].

Кыргызская Республика. В Законе «Об обращении лекарственных средств» НАП отнесена к надлежащим фармацевтическим практикам в сфере обращения лекарственных средств [7]. В НАП приведена классификация аптечных организаций по характеру их деятельности [12].

НАП Республики Казахстан и Республики Кыргызстан содержит общие требования к помещениям аптечных организаций: состав, размеры помещений должны соответствовать объему и характеру осуществляемой фармацевтической деятельности, но площади не нормированы [11, 12].

Республика Армения. В Законе «О лекарствах» установлен запрет на изготовление в аптеках инфузионных растворов, за исключением аптек, являющихся структурными подразделениями медицинских организаций, для которых в части этого также есть ограничения (разрешается изготавливать только те инфузионные растворы, которые не находятся в обращении в Республике Армения) [8]. Ввиду отсутствия НАП и в соответствии с названным законом,

основополагающими требованиями для функционирования ПА являются лицензионные требования.

Анализ законодательных актов, регулирующих обращение лекарственных средств, свидетельствует о наличии ПА и их необходимости во всех странах ЕАЭС, отдельно в видах аптек предусмотрены аптеки медицинских организаций. Во всех государствах, кроме Республики Армения, утверждены требования НАП, разнообразные по структуре. В республике Беларусь регламентирован комплекс помещений ПА, введены ограничения по расстоянию между аптеками и количеству аптек в одном капитальном строении. Площади помещений аптечных организаций в настоящее время не нормированы.

Список литературы

1. Мельникович Т. И., Новикова О. Л. Аптечное изготовление лекарственных средств: вчера и сегодня Вестник фармации. 2023. № 2(100). С. 34-41. DOI 10.52540/2074-9457.2023.2.34.
2. Шишова Л. И., Яруткин А.В., Багирова В. Л. Современные и перспективные фармакопейные требования к качеству экстенпоральных лекарственных препаратов: обзор регуляторных подходов / Регуляторные исследования и экспертиза лекарственных средств. 2024. Т. 14, № 4. С. 386-399. DOI 10.30895/1991-2919-2024-14-4-386-399.
3. Кугач В. В., Елисеенко Е. Ю. Классификация аптек (аптечных организаций, аптечных учреждений) в странах ЕАЭС, требования к их площадям и помещениям / Вестник фармации. 2020. № 3(89). С. 33-46.
4. Федеральный закон от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» [Электронный ресурс]. URL: <https://internet.garant.ru> (дата обращения 09.04.2026).
5. Закон Республики Беларусь 20.07.2006 № 161-З «Об обращении ЛС» [Электронный ресурс]. URL: <https://clck.ru/3Ng3Zv> (дата обращения 11.04.2026).
6. Кодекс Республики Казахстан «О здоровье народа и системе здравоохранения» (с изменениями и дополнениями по состоянию на 16.09.2025)

- [Электронный ресурс]. URL: <https://clck.ru/3Ng3Jp> (дата обращения 11.04.2026).
7. Закон Республики Кыргызстан от 12.01.2024 № 13 «Об обращении лекарственных средств» [Электронный ресурс]. URL: <https://cbd.minjust.gov.kg/4-5251/edition/1638/ru> (дата обращения 11.04.2026).
8. Закон Республики Армения от 17.05.2016 «О лекарствах» [Электронный ресурс]. URL: <https://www.arlis.am/hy/acts/177279> (дата обращения 11.04.2026).
9. Приказ Министерства здравоохранения Российской Федерации от 29.04.2025 № 259н «Об утверждении Правил надлежащей аптечной практики лекарственных препаратов для медицинского применения» [Электронный ресурс]. URL: <https://internet.garant.ru> (дата обращения 09.04.2026).
10. Постановление Министерства Здравоохранения Республики Беларусь от 27.12.2006 № 120 «Об утверждении надлежащей аптечной практики» [Электронный ресурс]. URL: <https://clck.ru/3Ng3cv> (дата обращения 11.04.2026).
11. Приказ и.о. Министра здравоохранения Республики Казахстан от 4 февраля 2021 года № ҚР ДСМ-15 «Об утверждении надлежащих фармацевтических практик», приложение 5 «Стандарт надлежащей аптечной практики (GPP)» [Электронный ресурс]. URL: <https://adilet.zan.kz/rus/docs/V2100022167#z6269> (дата обращения 11.04.2026).
12. Постановление Кабинета Министров Кыргызской Республики от 02.12.2024 № 720 «Об утверждении Правил надлежащей аптечной практики» [Электронный ресурс]. URL: <https://cbd.minjust.gov.kg/7-35713/edition/22237/ru> (дата обращения 11.04.2026).
13. Приказ Министерства здравоохранения РФ от 31.07.2020 № 780н «Об утверждении видов аптечных организаций» [Электронный ресурс]. URL: <https://internet.garant.ru> (дата обращения 09.04.2026).
14. МЗ РК составлен график перехода аптек на соответствие Стандарту GPP до 2025 года / Медсервис Плюс [Электронный ресурс]. URL: <https://clck.ru/3Q634M> (дата обращения 09.04.2026).
15. Приказ Министерства здравоохранения РФ от 22.05.2023 № 249н «Об утверждении правил изготовления и отпуска лекарственных препаратов для

медицинского применения аптечными организациями, имеющими лицензию на фармацевтическую деятельность» [Электронный ресурс]. URL: <https://internet.garant.ru> (дата обращения 09.04.2026).

16. Постановление Главного государственного санитарного врача РФ от 24.12.2020 № 44 «Об утверждении санитарных правил СП 2.1.3678-20 «Санитарно-эпидемиологические требования к эксплуатации помещений, зданий, сооружений, оборудования и транспорта, а также условиям деятельности хозяйствующих субъектов, осуществляющих продажу товаров, выполнение работ или оказание услуг» [Электронный ресурс]. URL: <https://internet.garant.ru> (дата обращения: 09.04.2026).

17. Постановление Главного государственного санитарного врача РФ от 28.01.2021 № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» [Электронный ресурс]. URL: <https://internet.garant.ru> (дата обращения: 09.04.2026).

18. Постановление Совета Министров Республики Беларусь 03.03.2020 г. № 130 «Об утверждении специфических санитарно-эпидемиологических требований» [Электронный ресурс]. URL: <https://clck.ru/3Q6DDU> (дата обращения: 11.04.2026).

ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.896

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ТРАНСФОРМАЦИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ: ОТ АВТОМАТИЗАЦИИ К ПЕРЕОПРЕДЕЛЕНИЮ ЗАНЯТОСТИ

Зиганшин Шамиль Эльмирович

Габдлхакова Лиана Фидановна

студенты

Научный руководитель: Семенова Дарья Вячеславовна,

старший преподаватель

ФГБОУ ВО «Уфимский государственный нефтяной технический университет»,

город Уфа

***Аннотация.** В статье предлагается интерпретация искусственного интеллекта (ИИ) как фактора не линейного технологического прогресса, а структурного сдвига в экономике. Показано, что его влияние проявляется через изменение логики организации труда и перераспределение функций между человеком и цифровыми системами. Обосновано, что ограничения развития ИИ связаны не столько с технологическими барьерами, сколько с ресурсной и инфраструктурной базой.*

The article proposes an interpretation of artificial intelligence (AI) as a factor of structural shift in the economy rather than linear technological progress. It is shown that its impact manifests through changes in the logic of work organization and the redistribution of functions between humans and digital systems. It is substantiated that the limitations of AI development are associated not so much with technological barriers as with resource and infrastructure constraints.

Ключевые слова: искусственный интеллект, трансформация экономики,

рынок труда, занятость, автоматизация, производительность труда, ресурсные ограничения

Keywords: *artificial intelligence, economic transformation, labor market, employment, automation, labor productivity, resource constraints*

Современное распространение искусственного интеллекта отличается от предыдущих этапов цифровизации тем, что он начинает затрагивать не отдельные операции, а целостные производственные процессы [2][3]. При этом внедрение происходит в условиях нестабильной макроэкономической среды, характеризующейся ростом затрат и ограниченностью ресурсов [5].

Это приводит к изменению роли технологий: ИИ используется не только для повышения эффективности, но и как механизм адаптации к внешнему давлению. В связи с этим некорректно рассматривать его влияние исключительно через призму сокращения рабочих мест. Более продуктивным является анализ изменений в структуре занятости и перераспределении функций между участниками производственного процесса [8].

Экономические оценки показывают, что ИИ уже встроен в глобальные процессы роста. По данным IDC, его вклад в мировую экономику к 2030 году может достигнуть 19,9–22,3 трлн долларов [1][12].

Существенным является не только масштаб, но и характер этого влияния. В частности, McKinsey оценивает потенциал ежегодного прироста производительности от генеративных технологий на уровне 4,4 трлн долларов [2]. При этом уровень их внедрения указывает на завершение экспериментальной стадии и переход к системному использованию [3].

Следовательно, ИИ функционирует как фактор, изменяющий саму производственную функцию экономики.

Распространённое представление о неизбежном исчезновении рабочих мест не подтверждается эмпирическими данными. Прогнозы Всемирного экономического форума указывают на положительный баланс занятости: количество создаваемых рабочих мест превышает число исчезающих [4][11].

Это означает, что ключевое изменение связано не с уменьшением

занятости, а с изменением её структуры и содержания.

На уровне отраслей трансформация проявляется через изменение параметров рынка труда. В ИТ-сфере наблюдается одновременное сокращение спроса на рабочую силу и рост предложения, что усиливает конкуренцию [8].

При этом финансовые показатели крупных компаний остаются устойчивыми [7], что позволяет сделать вывод: сокращения не обусловлены кризисом доходности, а связаны с оптимизацией структуры занятости.

Таким образом, формируется новая модель, в которой приоритет отдается высококвалифицированным специалистам, тогда как рутинные и начальные функции постепенно вытесняются.

Несмотря на активное развитие ИИ, его масштабирование сталкивается с объективными ограничениями. Ключевым из них является рост энергопотребления: по прогнозам, потребление электроэнергии дата-центрами более чем удвоится к 2030 году [5][13].

Это указывает на то, что развитие ИИ невозможно рассматривать изолированно от материальной базы. В отличие от распространённого представления о «нематериальности» цифровых технологий, их функционирование напрямую зависит от энергетических и инфраструктурных ресурсов [6].

Следовательно, дальнейшая экспансия ИИ будет определяться не только технологическими достижениями, но и возможностями их обеспечения.

Важным аспектом является взаимодействие ИИ и кризисных явлений. Сокращение издержек и пересмотр бизнес-моделей происходят в первую очередь под влиянием экономического давления, тогда как ИИ выступает инструментом реализации этих изменений [2].

Компании переходят от экстенсивного роста к повышению эффективности, что выражается в сокращении избыточных функций и автоматизации процессов. В результате формируется более компактная организационная структура, ориентированная на максимизацию производительности.

Развитие ИИ приводит к переходу от автоматизации отдельных задач к автоматизации процессов управления. Агентные системы способны выполнять

последовательности действий, что снижает необходимость постоянного участия человека.

Это изменяет саму природу труда: основная роль работника смещается в сторону постановки задач, интерпретации результатов и контроля [9][10].

Таким образом, происходит не только количественное, но и качественное изменение занятости, связанное с усложнением профессиональных требований.

Проведённый анализ позволяет сделать ряд обобщений.

Во-первых, ИИ является значимым фактором макроэкономического развития и влияет на структуру глобального роста [1] [2]. Во-вторых, его воздействие на рынок труда проявляется через перераспределение функций, а не через сокращение занятости [4]. В-третьих, компании адаптируют кадровую политику, усиливая селективность найма и повышая требования к квалификации [8]. В-четвёртых, развитие технологий ограничено ресурсными факторами, прежде всего энергетическими [5].

Обобщая, можно утверждать, что ИИ выступает не столько инструментом автоматизации, сколько фактором перехода к новой модели экономики, в которой меняются принципы организации труда и производства.

Список литературы

1. McKinsey & Company. The Economic Potential of Generative AI: The Next Productivity Frontier / McKinsey Global Institute. – New York: McKinsey & Company, 2023. – 124 p.

2. McKinsey & Company. The State of AI: 2024 and Beyond / McKinsey Digital. – New York: McKinsey & Company, 2024. – 96 p.

3. International Energy Agency. Data Centre Power Demand: Outlook to 2030 / IEA. – Paris: IEA Publications, 2025. – 87 p.

4. Рынок труда в ИТ: спрос и предложение в 2025 году [Электронный ресурс] / РБК. – 2025. – 10 апреля. – Режим доступа: <https://www.rbc.ru/technology/12345678> (дата обращения: 10.04.2026).

5. IDC. Worldwide AI Spending Guide / International Data Corporation. –

Framingham: IDC, 2024. – 58 p.

6. IDC / LinkedIn. AI Economic Impact: Global Forecast to 2030 / IDC & LinkedIn. – Framingham: IDC, 2024. – 112 p.

7. World Economic Forum. Future of Jobs Report 2025 / WEF. – Geneva: World Economic Forum, 2025. – 210 p.

8. Coursera. WEF Future of Jobs Report 2025: Key Insights for Lifelong Learning / Coursera Blog [Электронный ресурс]. – 2025. – Режим доступа: <https://blog.coursera.org/wef-future-of-jobs-2025> (дата обращения: 11.04.2026).

9. Отчетность компаний за 2024 год: ключевые показатели [Электронный ресурс] / Коммерсантъ. – 2025. – 15 марта. – Режим доступа: <https://www.kommersant.ru/doc/1234567> (дата обращения: 17.04.2026).

10. Nature. Data Centre Energy Use: Global Trends and Projections / Nature Portfolio / Nature. – 2025. – Vol. 628, No. 3. – P. 45–52.

11. IEA 4E. Data Centre Energy Review 2025 / IEA 4E Programme. – Paris: IEA, 2025. – 73 p.

12. СберПро. Искусственный интеллект в промышленности: практика внедрения / СберПро. – М.: СберПро, 2024. – 65 с.

13. Korus Consulting. Применение ИИ в промышленности России: обзор 2024 / Korus Consulting. – СПб.: Korus, 2024. – 42 с.

УДК 62

УЯЗВИМОСТИ СИСТЕМ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ: АТАКИ НА ОБУЧЕНИЕ И ВНЕДРЕНИЕ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ

Ивинских Игорь Валерьевич**Кияшко Милана Антоновна**

магистранты

Научный руководитель: Газизов Андрей Равильевич,

канд. пед. наук, заведующий кафедрой информационная безопасность

в вычислительных системах и сетях, доцент

Донской государственной технической университет,

город Ростов-на-Дону

***Аннотация.** В статье изучено внедрение систем машинного обучения (МО) в задачи защиты информации (ЗИ), такие как обнаружение вторжений и анализ вредоносного ПО, создает новые векторы атак. Модели МО уязвимы к специально сконструированным состязательным воздействиям, что ставит под угрозу надежность защитных механизмов. Целью статьи является анализ ключевых уязвимостей МО-моделей в контексте ЗИ, систематизация атак и оценка современных методов противодействия. В работе проведен анализ и классификация основных типов состязательных атак: на этап обучения (poisoning-атаки), направленных на искажение данных для компрометации модели, и на этап эксплуатации (evasion-атаки), цель которых — обман обученной модели с помощью специально созданных входных данных. Рассмотрены методы защиты, включающие повышение устойчивости моделей, детектирование аномальных входных данных и мониторинг целостности данных. Выводы о критической необходимости интеграции механизмов защиты от*

состязательных атак в процессы разработки и эксплуатации ML-систем для ЗИ.

The introduction of machine learning (MO) systems into information security tasks, such as intrusion detection and malware analysis, creates new attack vectors. MO models are vulnerable to specially designed competitive influences, which jeopardizes the reliability of protective mechanisms. The purpose of the article is to analyze the key vulnerabilities of MO models in the context of AI, systematize attacks and evaluate modern methods of counteraction. The paper analyzes and classifies the main types of adversarial attacks: the training stage (poisoning attacks) aimed at distorting data to compromise the model, and the operation stage (evasion attacks), the purpose of which is to deceive the trained model using specially created input data. Protection methods are considered, including increasing the stability of models, detecting abnormal input data, and monitoring data integrity. Conclusions about the critical need to integrate protection mechanisms against adversarial attacks into the development and operation of ML systems for AI.

Ключевые слова: *системы машинного обучения, информационная безопасность, состязательные атаки, poisoning-атаки, adversarial examples, устойчивость моделей, обнаружение вторжений, защита информации*

Keyword: *machine learning systems, information security, adversarial attacks, poisoning attacks, adversarial examples, model resilience, intrusion detection, information protection*

Актуальность темы. В последние годы наблюдается стремительная интеграция методов искусственного интеллекта и машинного обучения (ИИ/ML) в ядро систем защиты информации (ЗИ). Эти технологии лежат в основе современных SIEM-систем, систем обнаружения и предотвращения вторжений (IDS/IPS), решений класса «антивирусы нового поколения» (NGAV), средств предотвращения утечек данных (DLP) и биометрической аутентификации. Однако возникает парадокс: машинное обучение, будучи мощным инструментом для выявления сложных угроз, одновременно формирует новую, недостаточно изученную поверхность для атак. Проблема заключается в том, что сами ML-модели,

используемые для защиты, обладают внутренними уязвимостями и подвержены целенаправленным состязательным воздействиям. Успешная атака на такую модель может привести к полному обходу механизмов безопасности, делая всю систему защиты неэффективной и создавая критические риски.

Степень изученности проблемы. Фундаментальные основы уязвимостей ML и состязательных атак были заложены в работах таких зарубежных исследователей, как В. Biggio, N. Papernot, I. Goodfellow и других, которые сформулировали ключевые концепции poisoning-атак и adversarial examples. Отечественные авторы такие как Петренко В.И., Тебуева Ф.Б. и другие из сектора информационной безопасности также активно развивают данную тему. Обзорным исследованием, таким как работа «Taxonomy of Attacks on Machine Learning in Cybersecurity» авторов Н. S. Anderson et al, удалось систематизировать угрозы. Однако, как справедливо отмечается в обзоре «Adversarial Machine Learning in Network Intrusion Detection Systems» А. Khraisat, большинство фундаментальных исследований носят теоретический характер или сфокусированы на домене компьютерного зрения. Применение существующих таксономий и методов противодействия к специфическим, критически важным задачам ЗИ (анализ сетевого трафика, статический и динамический анализ вредоносного ПО) требует отдельного, прикладного анализа с учетом особенностей данных и ограничений реальных систем.

Систематизация угроз безопасности систем машинного обучения является необходимым условием для разработки эффективных контрмер. В контексте защиты информации (ЗИ) такая классификация требует адаптации общих таксономий состязательного машинного обучения к специфике предметной области. В основу предлагаемой классификации положены фундаментальные критерии, сформулированные в работах по безопасности ML [2, 10], и их развитие в прикладных исследованиях, посвященных уязвимостям киберфизических систем и систем анализа данных [23, 16].

Традиционно угрозы разделяются по фазе жизненного цикла модели, на которую они направлены: атаки на этапе обучения и на этапе вывода. Более

детальная градация осуществляется согласно цели нарушения базовых свойств безопасности: целостности, доступности или конфиденциальности модели и данных [2]. Наконец, принципиальное значение имеет уровень информированности злоумышленника, определяемый как white-box или black-box сценарий [10].

Атаки на этапе обучения. Наиболее опасными в данном классе являются атаки на целостность обучающих данных. К ним относятся poisoning-атаки, целью которых является внесение скрытых искажений в тренировочный набор для ухудшения обобщающей способности или создания целенаправленных «слепых зон» в модели [3]. Частным, но критически важным случаем выступают backdoor- или троянские атаки, при которых модель корректно функционирует на большинстве данных, но выполняет заданный злоумышленником сценарий при предъявлении образца со скрытым триггером [6]. В области ЗИ подобные атаки могут быть направлены на компрометацию систем обнаружения вторжений или антивирусных решений нового поколения, что подтверждается исследованиями уязвимости алгоритмов глубокого обучения к подобным воздействиям [25, 32].

Атаки на этапе вывода. Основным вектором атак на развернутую модель является генерация состязательных примеров- входных данных, модифицированных с помощью малозаметных возмущений, что приводит к целенаправленной ошибке классификации или регрессии. Механизмы генерации варьируются от быстрых однократных методов, таких как FGSM [5], до итеративных и оптимизационных подходов, подобных PGD. В условиях black-box доступа эффективность демонстрируют атаки на основе переноса и методы, строящие суррогатную модель [9]. Применительно к задачам ЗИ это означает возможность обхода ML-детекторов путем аддитивного искажения признакового пространства сетевого трафика, байт-кода исполняемых файлов или иных анализируемых объектов [16].

Атаки на конфиденциальность. Данный класс угроз ставит под риск не функциональность, а приватность модели и данных. Membership inference attack позволяет установить факт использования конкретного конфиденциального

образца (например, персональных данных или служебной информации) в тренировочном наборе целевой модели [11]. Model extraction attack направлен на кражу интеллектуальной собственности – восстановление архитектуры и параметров модели через анализ ее ответов на последовательность запросов [12]. Обе атаки создают значительные риски для коммерческих систем ЗИ, так как ведут к утечке критической информации и облегчают подготовку последующих evasion-атак, что актуализирует вопросы защиты ML-моделей в рамках правового и технического регулирования.

Таким образом, многообразие векторов атак на системы машинного обучения в ЗИ требует комплексного подхода к безопасности на всех этапах их жизненного цикла – от сбора данных до промышленной эксплуатации.

Современная парадигма обеспечения безопасности систем машинного обучения (МО) предполагает комплексный подход, реализуемый на всех этапах жизненного цикла модели. Методы противодействия дифференцируются в зависимости от фазы, на которую направлена угроза, и требуют адаптации к конкретным условиям эксплуатации в системах защиты информации (ЗИ).

Ключевым направлением является повышение устойчивости модели на этапе ее формирования. Техники очистки данных и применение робастной статистики направлены на фильтрацию потенциально отравленных образцов путем выявления семантических или статистических аномалий в тренировочном наборе [3]. Более активной стратегией выступает состязательное обучение, при котором в процесс оптимизации явно включаются состязательные примеры, что позволяет модели обучаться корректно классифицировать искаженные входные данные. Несмотря на доказанную эффективность против evasion-атак, метод может приводить к снижению точности на чистых данных [8].

Для противодействия атакам на конфиденциальность, таким как membership inference, применяются методы дифференциальной приватности. Внедрение контролируемого случайного шума в градиенты (DP-SGD) обеспечивает формальные математические гарантии невозможности определения факта присутствия конкретного образца в обучающей выборке [1]. Архитектурным

решением, снижающим риски централизованного сбора данных, является федеративное обучение. В этой парадигме модель обучается децентрализованно, а на сервер передаются только обновления параметров, что усложняет проведение масштабных poisoning-атак [7].

Защита развернутой модели от evasion-атак часто реализуется через модификацию входного конвейера. Методы трансформации и рандомизации входа, такие как случайное изменение разрешения или добавление шума, могут эффективно нейтрализовать слабо сконструированные adversarial-возмущения [13]. Более специализированным подходом является детектирование состязательных примеров с помощью дополнительных классификаторов. Как показано в работе Чехонина Е. А. и др., эффективным методом является построение детектора на основе анализа метрик уверенности модели и применения алгоритмов машинного обучения для классификации легитимных и состязательных входов [32].

Повышение внутренней устойчивости модели достигается за счет архитектурных и алгоритмических решений. Использование ансамблей разнородных моделей усложняет задачу атакующего. Дистилляция знаний, при которой компактная модель- «ученик» обучается имитировать выходы более крупной модели-«учителя», также может способствовать сглаживанию пространства решений. Перспективным направлением является использование методов формальной верификации, позволяющих доказывать отсутствие adversarial examples в заданной окрестности входного пространства для обеспечения гарантированной безопасности критических систем.

Технические методы должны быть подкреплены организационными мерами в рамках защищенного MLOps-конвейера. Безопасность ML-конвейера (MLOps Security) включает в себя контроль целостности данных, верификацию кода обучения, а также непрерывный мониторинг дрейфа данных и производительности модели, что может служить индикатором успешной атаки. Реализация принципа минимальных привилегий для доступа к API инференса и параметрам модели ограничивает поверхность для проведения атак на извлечение модели. Комплексное применение перечисленных стратегий, адаптированных к

требованиям конкретных систем ЗИ, позволяет создавать более устойчивые и надежные решения.

Практическая имплементация методов защиты машинного обучения в системах информационной безопасности требует проведения сравнительного анализа, основанного на ключевых критериях эффективности, производительности и применимости. Такой анализ позволяет сформулировать адресные рекомендации, ориентированные на конкретные классы задач и типичные сценарии эксплуатации.

В качестве базовых критериев для сравнения методов защиты целесообразно рассматривать их специализацию относительно фазы атаки (обучение или вывод), предоставляемый уровень гарантий, вычислительную нагрузку, влияние на исходную точность работы модели, а также интеграционную сложность в существующие технологические процессы (MLOps).

Так, состязательное обучение, несмотря на доказанную эффективность против evasion-атак, влечет значительное увеличение вычислительных затрат на этапе обучения и, как следствие, может приводить к снижению точности классификации на «чистых» данных. Этот компромисс между точностью и устойчивостью подробно исследуется в работе Евдокимовой, которая анализирует адаптацию методов генерации состязательных примеров для задач сетевой безопасности [18].

Методы детектирования состязательных примеров, например, подход на основе анализа статистики предсказаний или скрытых представлений модели, характеризуются относительно низкими накладными расходами в режиме инференса. Однако их эффективность критически зависит от способности детектора к обобщению на новые, неизвестные типы атак. Исследование Козловой посвящено именно этой проблеме и предлагает метод комбинирования нескольких детекторов для снижения уровня ложных срабатываний [24].

Техники, основанные на дифференциальной приватности, такие как DP-SGD, предлагают строгие формальные гарантии против атак на раскрытие информации, но вводят фундаментальный компромисс между приватностью и

полезностью модели. Как показано в работе Михайлова и др., применение DP в задачах анализа сетевого трафика требует тщательного подбора параметров шума для сохранения приемлемой точности детектирования аномалий [27].

Архитектурные подходы, включая ансамблирование и дистилляцию, повышают сложность системы для атакующего, но одновременно увеличивают и операционные издержки. Практическая эффективность построения ансамблей из разнородных моделей для защиты систем обнаружения вторжений эмпирически подтверждена в исследовании Бербер [15].

На основе проведенного анализа можно сформулировать следующие практические рекомендации, структурированные по классам задач защиты информации.

Для систем, функционирующих в условиях потенциального отравления обучающих данных (например, при использовании публично доступных датасетов угроз), приоритетной является организация многоэтапной процедуры валидации и очистки данных. Данная процедура должна быть дополнена применением состязательного обучения для повышения общей робастности модели, что соответствует принципу упреждающей защиты [19].

В приложениях, обрабатывающих конфиденциальные данные, обязательным элементом проектирования является внедрение механизмов обеспечения приватности. Для централизованных сценариев оптимальным считается применение алгоритмов дифференциальной приватности с тщательной калибровкой параметров. В распределенных архитектурах, как отмечает коллектив авторов в обзоре по федеративному обучению для кибербезопасности, следует рассматривать федеративные схемы как метод минимизации рисков утечки исходных данных [17].

Для систем реального времени, таких как межсетевые экраны нового поколения (NGFW) или детекторы вредоносного ПО на конечных точках, где критична задержка принятия решения, использование ресурсоемких методов защиты на этапе инференса недопустимо. В данном контексте рекомендованы легковесные методы, такие как случайная предобработка входных данных или

использование высокоэффективных «сторожевых» моделей-детекторов.

Ключевым стратегическим принципом является реализация подхода «глубокой эшелонированной обороны». Наиболее устойчивая архитектура формируется путем комбинации взаимодополняющих методов, действующих на разных уровнях пайплайна машинного обучения. Это может включать: защиту данных и модели на этапе обучения, усиление модели, контроль входного трафика и непрерывный мониторинг производственного конвейера (MLOps). Такой многослойный подход, адаптированный под профиль угроз конкретной системы, максимально затрудняет для злоумышленника достижение конечной цели атаки.

Проведённое исследование демонстрирует, что уязвимости систем машинного обучения, подверженные целенаправленным состязательным воздействиям, формируют значимый класс современных киберугроз. Эти угрозы напрямую подрывают надежность автоматизированных систем защиты информации, таких как системы обнаружения вторжений нового поколения, платформы для анализа вредоносного ПО и средства биометрической аутентификации, перенося конфликт в область эксплуатации алгоритмических уязвимостей. Наибольшую операционную сложность представляют атаки на этапе обучения, в частности, сложные poisoning-атаки и внедрение троянских закладок, поскольку их последствия проявляются только в определённых условиях эксплуатации модели и могут длительное время оставаться необнаруженными, что отмечается в исследованиях, посвящённых скрытым угрозам для нейросетевых классификаторов [26].

Сравнительный анализ методов противодействия подтверждает отсутствие универсального решения и выявляет устойчивые компромиссы между уровнем защищённости, производительностью системы и точностью работы модели на легитимных данных. Эффективность таких методов, как состязательное обучение, детектирование вредоносных примеров на основе анализа мета-признаков, применение ансамблей моделей и использование дифференциальной приватности, существенно зависит от контекста задачи и архитектурных ограничений. Это обуславливает необходимость разработки адаптивных,

многоуровневых систем защиты, реализующих принцип глубокой эшелонированной обороны для MLOps-конвейеров.

Таким образом обеспечение безопасности машинного обучения является не дополнительной опцией, а обязательным требованием при проектировании и эксплуатации интеллектуальных систем в области защиты информации. Устойчивость к состязательным атакам должна закладываться на архитектурном уровне и контролироваться на всех этапах жизненного цикла модели — от сбора данных и обучения до промышленного внедрения, и мониторинга. Дальнейший прогресс в этой области возможен только на основе конвергенции знаний из машинного обучения, криптографии, теории сложности систем и практической кибербезопасности.

Список литературы

1. Abadi, M. et al. Deep learning with differential privacy / Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.
2. Barreno, M., Nelson, B., Sears, R., Joseph, A. D., & Tygar, J. D. Can machine learning be secure? / Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS). 2010.
3. Biggio, B., Nelson, B., & Laskov, P. Poisoning attacks against support vector machines / Proceedings of the International Conference on Machine Learning (ICML). 2012.
4. Carlini, N., & Wagner, D. Towards evaluating the robustness of neural networks / Proceedings of the IEEE Symposium on Security and Privacy (S&P). 2017.
5. Goodfellow, I. J., Shlens, J., & Szegedy, C. Explaining and harnessing adversarial examples / Proceedings of the International Conference on Learning Representations. 2015.
6. Gu, T., Liu, K., Dolan-Gavitt, B., & Garg, S. BadNets: Evaluating backdoor- ing attacks on deep neural networks / IEEE Access. 2019.
7. Konečný, J. et al. Federated learning: Strategies for improving communication efficiency / arXiv preprint arXiv:1610.05492. 2016.

8. Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. Towards deep learning models resistant to adversarial attacks / Proceedings of the International Conference on Learning Representations (ICLR). 2018.
9. Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. Practical black-box attacks against machine learning / Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS). 2017.
10. Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. The limitations of deep learning in adversarial settings / Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P). 2016.
11. Shokri, R., Stronati, M., Song, C., & Shmatikov, V. Membership inference attacks against machine learning models / Proceedings of the IEEE Symposium on Security and Privacy (S&P). 2017.
12. Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. Stealing machine learning models via prediction APIs / Proceedings of the USENIX Security Symposium. 2016.
13. Xie, C. et al. Mitigating adversarial effects through randomization / International Conference on Learning Representations. 2018.
14. Аветисян А. И. Кибербезопасность в контексте искусственного интеллекта / Вестник Российской академии наук. 2022. Т. 92, № 12. С. 1119-1123
15. Бербер Д. В., Лапоница О. Р. Разработка подходов к увеличению устойчивости моделей машинного обучения для обнаружения распределенных атак отказа обслуживания / International Journal of Open Information Technologies. 2025
16. Берешполов И. С., Кравченко Ю. А., Слепцов А. Г. Алгоритм кластеризации данных для защиты конфиденциальной информации в сети Интернет / Известия ЮФУ. Технические науки. 2023. № 3
17. Виноградова Е., Головин Е. Метрики качества алгоритмов машинного обучения в задачах классификации / Научная сессия ГУАП. — 2017. — с. 202—206
18. Евдокимова Т. С. Влияние методов расширения наборов данных на качество обучения нейросетевых моделей. Адаптивный подход расширения

наборов данных / Инженерный вестник Дона. 2024. № 8.

19. Евдокимова Т. С., Шлеймович М. П. Оценка эффективности метода расширения наборов данных на основе глубокого обучения с подкреплением / ИВД. 2025.

20. Запечников С. В. Информационная безопасность, искусственный интеллект, системы распределенного реестра: достижения, проблемы, перспективы / Вестник современных цифровых технологий. 2023. № 14. С. 20-28

21. Запечников С. В. Модели и алгоритмы конфиденциального машинного обучения / Безопасность информационных технологий. 2020. Т. 27, № 1. С. 51-67

22. Каскырбаева К. С. Применение глубоких нейронных сетей для обнаружения вредоносного программного обеспечения / Вестник науки. 2025.

23. Кафтанников И. Л., Парасич А. В. Особенности применения деревьев решений в задачах классификации / Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. — 2015

24. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности / Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2023

25. Ли К., Парк С., Джонсон Т. Применение сверточных нейронных сетей для статического анализа вредоносного ПО. Труды международной конференции по информационной безопасности, 145-159. 2023.

26. Менисов А. Б. Технологии искусственного интеллекта и кибербезопасность: монография. Москва: Ай Пи Ар Медиа, 2022. 133 с.

27. Михайлов А. Н. Обнаружение аномалий в сетевом трафике с использованием методов машинного обучения / Вестник науки. 2024.

28. Сухомлин В. А., "Модель цифровых навыков кибербезопасности 2020." Современные информационные технологии и ИТ-образование 16.3 (2020): 695-710.

29. Топольский Н. Г., Вилисов В. Я. Методы, модели и алгоритмы в системах безопасности: машинное обучение, робототехника, страхование, риски, контроль. Москва: ООО «Издательский Центр РИОР», 2021.

30. Чен Л., Парк С. Объяснимый ИИ для систем обнаружения вторжений: повышение доверия к решениям машинного обучения. Международный журнал сетевой безопасности, 21(3), 189-204. 2023

31. Черниговский А.В., Кривов М. В. Нейронные сети как инструмент анализа сетевого трафика / Вестник Ангарского государственного технического университета. 2019. № 13.

32. Чехонина Е. А., Костюмов В. В. Обзор состязательных атак и методов защиты для детекторов объектов / International Journal of Open Information Technologies. 2023.

УДК 623.85/621.43.057.2

РАЗРАБОТКА МОДЕЛЕЙ ДИЗЕЛЬНОГО ТОПЛИВА ДЛЯ ОЦЕНКИ СТАБИЛЬНОСТИ ЕГО СВОЙСТВ ПРИ ХРАНЕНИИ С МОРСКОЙ ВОДОЙ

Нелюбов Дмитрий Владимирович

к.т.н., старший научный сотрудник

ФАУ «25 ГосНИИ химмотологии Минобороны России»,

город Москва

***Аннотация.** Проанализированы данные о содержании ароматических углеводов, молекулярно-массовом распределении n-алканов и среднем дипольном моменте топлива ДТ-Л-К5 по ГОСТ 32511 для оценки его диспергирующей способности по отношению к функциональным присадкам, а также склонности к образованию биозагрязнений при контакте с морской водой. Установлено, что для обеспечения приемлемой точности оценки влияния функциональных присадок на образование биозагрязнений при контакте топлива с морской водой необходимо применение модельных смесей, состоящих из предельного углеводорода, соответствующего среднему по массе n-алкану в составе дизельного топлива и ароматического углеводорода, не подавляющего биологическую активность в морской воде с добавлением функциональных присадок в типичном диапазоне их концентраций. Обоснован состав модельных смесей, применение которого обеспечивает возможность исследования вышеперечисленных свойств ДТ-Л-К5 по ГОСТ 32511 с необходимой точностью.*

***Abstract.** The data on the content of aromatic hydrocarbons, the molecular-weight distribution of n-alkanes, and the average dipole moment of DT-L-K5 fuel according to GOST 32511 were analyzed to assess its dispersing ability with respect to functional additives, as well as its tendency to form bio-contaminations upon contact*

with seawater. It was established that, to ensure acceptable accuracy in evaluating the effect of functional additives on the formation of bio-contaminations during fuel contact with seawater, it is necessary to use model mixtures. These mixtures should consist of: a saturated hydrocarbon corresponding to the average n-alkane by mass in the diesel fuel composition; an aromatic hydrocarbon that does not inhibit biological activity in seawater; functional additives at their typical concentration ranges. The composition of the model mixtures has been substantiated, and its application enables the investigation of the aforementioned properties of DT-L-K5 fuel according to GOST 32511 with the required accuracy.

Ключевые слова: дизельное топливо, биозагрязнения, сохраняемость

Keywords: diesel fuel, bio-contamination, storage ability

В числе задач, решаемых в рамках исследований стабильности дизельных топлив (далее – ДТ) при их хранении в контакте с морской водой, не описанных в работе [1], было установление наличия зависимостей, определяемых изменением содержания промотора воспламенения (далее – ПВ), поверхностно-объемного соотношения контактирующих фаз, а также содержания микроорганизмов в морской воде на качество ДТ. Для этого рассматривалась возможность применения однокомпонентной базовой фракции гидроочистки ДТ.

Полученные в работе [1] данные об образовании биозагрязнений в воде и топливе указывают на то, что топлива ДТ-Л-К5, идентичные по содержанию функциональных присадок и близкие по компонентному составу базовой фракции существенно отличаются по интенсивности образования биозагрязнений в морской воде, определяемой по ASTM D7978, при её хранении в контакте с топливами (рисунок 1), а также влиянием этих биозагрязнений на прокачиваемость топлив. Так коэффициент фильтруемости, определяемый по ГОСТ 19006, у ДТ-Л-К5 производства НПЗ № 1 при хранении в контакте с морской водой в течение 12 мес. ухудшился на 30 %, а у ДТ-Л-К5 производства НПЗ № 2 – в 2,7 раз и составил 3,5, что выше установленной нормы.

Такое различие в микробиологической устойчивости ДТ-Л-К5 может объясняться различиями в их углеводородном составе и содержании гетероатомных

соединений. Так, в обзоре [2] приведены сведения о том, что окисление микроорганизмами парафиновых и циклопарафиновых углеводородов ДТ осуществляется по различным механизмам, а согласно [3] продукты жизнедеятельности микроорганизмов могут существенно отличаться в зависимости от индивидуальных особенностей химического состава питательной среды (топлива). Поэтому применение базовой фракции ДТ, углеводородный состав которой обладает микробиологической устойчивостью вблизи нижнего, либо верхнего предела её определения применяемым методом, осложнит установление каких-либо изменений в биозагрязнённости топлива и воды с учётом невысокой точности соответствующих методов. Вместе с тем углеводородный состав базовой фракции ДТ со средним уровнем микробиологической устойчивости зачастую не является представительным.

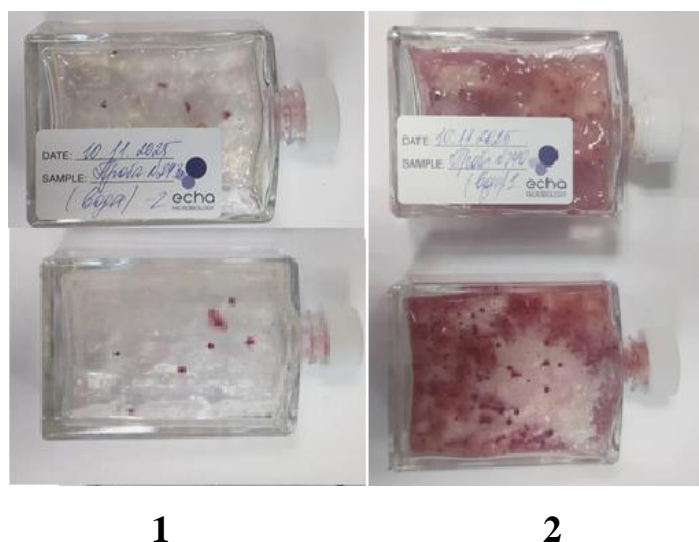


Рисунок 1 – Результаты определения содержания жизнеспособных микроорганизмов в морской воде по ASTM D7978-25 после 12 мес. контакта с топливами ДТ-Л-К5 производства: 1 – НПЗ № 1 (70 КОЕ/мл); 2 – НПЗ № 2 (не более 1000 КОЕ/мл)

С учётом изложенного, для оценки влияния содержания ПВ и изменения поверхностно-объемного соотношения контактирующих фаз на образование биозагрязнений в ДТ использовались модельные углеводородные смеси (далее – МУС), базовая основа которых состоит из индивидуальных химических соединений, содержащихся в ДТ-Л-К5, которые могут являться питательной средой и

не препятствовать развитию микроорганизмов, содержащихся в морской воде. При этом показатели, определяющие дисперсионную способность базовой основы МУС по отношению к функциональным присадкам для ДТ, а именно дипольный момент и средняя молекулярная масса должны быть близки к средним значениям содержания аналогичных групп соединений в ДТ-Л-К5 с целью исключения несвойственной ДТ-Л-К5 (как установлено в работе [1]) экстракции присадок водой.

Согласно обзору [4] н-алканы являются наиболее склонными к биодegradации углеводородами. Среди н-алканов лучше всего усваиваются микроорганизмами низкомолекулярные соединения в ряду от C_{14} до C_{20} .

На рисунке 2 молекулярно-массовое распределение н-алканов в летнем ДТ по данным хроматографии с пламенно-ионизационным детектированием.

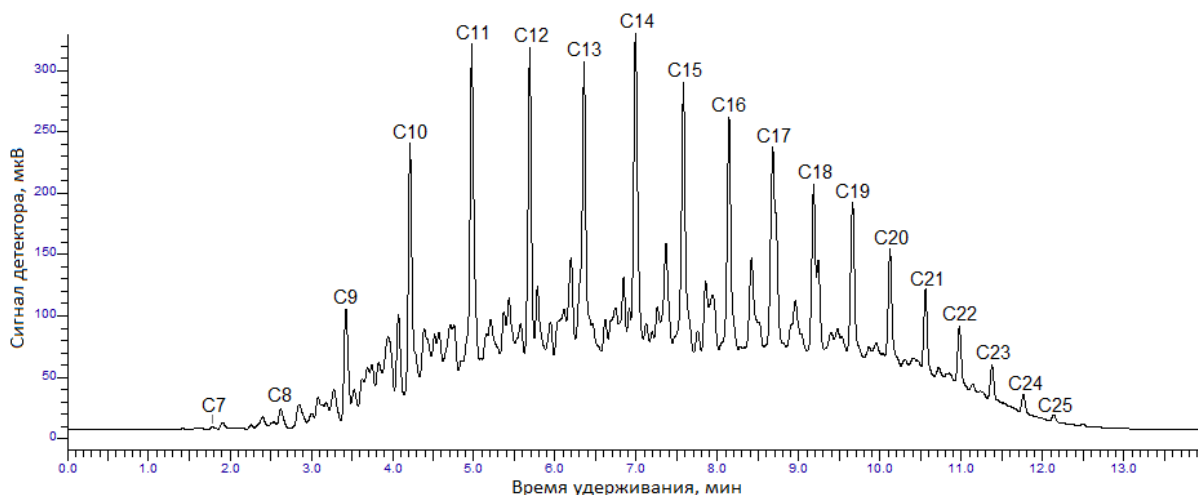


Рисунок 2 – Хроматограмма пробы летнего ДТ

Анализ данных рисунка 2, а также аналогичных данных, приведённых в диссертации [5], показал, что среднее значение молекулярной массы н-алканов, присутствующих в летних ДТ, соответствует додекану, однако в связи с отсутствием данных о его склонности к биодegradации был использован более доступный и располагающийся в средней области молекулярно-массового распределения алканов в ДТ – н-гексадекан (цетан).

Дипольный момент дистиллятных фракций нефти малозначительно отличается от нуля (0,5-0,8 Д) лишь благодаря содержанию аренов. Поэтому для

обеспечения необходимой дисперсионной способности смесей в качестве второго компонента МУС использовали ароматический углеводород.

Согласно обзору [3] моноароматические углеводороды являются токсинами для большей части морской микрофлоры, в отличие от ди- и триароматики. При этом их склонность к биодegradации отдельными штаммами микроорганизмов соответствует 1-метилнафталину [5], что стало причиной применения 1-метилнафталина с дипольным моментом 0,5 Д [7] в МУС.

Анализ данных о содержании ароматических углеводородов в промышленных образцах ДТ-Л-К5 за последние 5 лет показал, что среднее значение данного показателя составляет 18 %. Поэтому состав базовой основы МУС был определён в виде смеси цетана и 1-метилнафталин (72 % к 18 % масс).

В составе ДТ-Л-К5 применяются ПВ на основе 2-этилгексилнитрата и ПП на основе дистиллированных жирных кислот талового масла. Содержание ПВ в ДТ-Л-К5 варьируется от 0 до 0,2 % масс. Концентрацию ПП в МУС установили по среднему значению её содержания в ДТ-Л-К5 – 0,04 % масс.

Вышеизложенные доводы позволили разработать МУС, предназначенные для исследования влияния содержания ПВ, поверхностно-объемного соотношения контактирующих фаз, а также содержания микроорганизмов в морской воде на качество ДТ.

Список литературы

1. Нелюбов Д. В., Береснева О. В., Чернышёва А.В. и др. Исследование стабильности дизельных топлив при их хранении в контакте с морской водой. Труды 25 ГосНИИ МО РФ. 2025; 63:74–89.
2. Khalid F. E., Lim Z. S., Sabri S., et al. Bioremediation of diesel contaminated marine water by bacteria: review and bibliometric analysis. J Mar Sci Eng. 2021; 9(2):155. doi:10.3390/jmse9020155
3. Bobić V, Beer-Romac I, Štajduhar L. The diesel and biodiesel fuel biodegradation testing for supply chain control and quality preservation. Goriva i Maziva. 2015;54(2):123–137.

4. Тимергазина И. Ф., Переходова Л. С. Проблема биологического окисления нефти и нефтепродуктов микроорганизмами. Нефтегазовая Геология. 2012;7(1). 5. Синюта В. Р. Контроль свойств дизельных топлив. Дисс... канд техн наук. Красноярск: СибФУ; 2019. 124 с.

6. Щербаченко Л. А., Карнаков В. А., Марчук С. Д. Определение дипольного момента методом Дебая. Иркутск: ИГУ; 2005. 16 с.

7. Reid R, Prausnitz J, Sherwood T. Свойства газов и жидкостей. 3-е изд. Ленинград: Химия; 1982. 592 с.

ЭКОНОМИЧЕСКИЕ НАУКИ

УДК 33

AGILE-МЕТОДОЛОГИИ В РОССИЙСКИХ СТАРТАПАХ: ЭКОНОМИЧЕСКИЕ ФАКТОРЫ ВЫБОРА И РЕЗУЛЬТАТИВНОСТИ

Канзепаров Руслан Ринатович

аспирант кафедры менеджмента

НОЧУ ВО «Московский финансово-промышленный университет «Синергия»,
город Москва

Научный руководитель: Семенова Алла Анатольевна,

доктор экономических наук, профессор кафедры менеджмента

АНО ВО «Российский Новый университет» (РосНОУ),

город Москва

***Аннотация.** В статье исследуется влияние гибких методологий на результативность управления российскими стартапами. Показано, что практическая ценность Scrum, Kanban и Lean Startup зависит от стадии развития проекта, структуры команды и характера управленческих ограничений. Обосновано, что для молодой компании ключевыми критериями выбора методологии выступают скорость проверки гипотез, прозрачность координации, стоимость изменения решения и качество взаимодействия с клиентом. Сделан вывод о целесообразности последовательного применения гибких инструментов: Lean Startup на этапе поиска жизнеспособной бизнес-модели, Kanban при росте операционной нагрузки и Scrum при усложнении командной координации.*

***Abstract.** The article investigates the impact of agile methodologies on the managerial effectiveness of Russian startups. It is shown that the practical value of Scrum, Kanban and Lean Startup depends on the stage of venture development, team structure and the nature of managerial constraints. The paper argues that for a young company the key criteria for choosing a methodology are the speed of hypothesis validation,*

transparency of coordination, the cost of changing decisions and the quality of customer interaction. It is concluded that agile tools should be applied sequentially: Lean Startup at the stage of searching for a viable business model, Kanban when operational workload increases, and Scrum when team coordination becomes more complex.

Ключевые слова: *гибкие методологии, Agile, стартап, Scrum, Kanban, Lean Startup, управленческая результативность, проектное управление, российское предпринимательство*

Keywords: *agile methodologies, Agile, startup, Scrum, Kanban, Lean Startup, managerial effectiveness, project management, Russian entrepreneurship*

Стартап в современной экономике выступает не как уменьшенная копия зрелой компании, а как временная предпринимательская организация, одновременно формирующая продукт, проверяющая гипотезы о клиенте и ищущая устойчивую бизнес-модель. Поэтому для него особенно значим выбор управленческого подхода: если крупный бизнес опирается на стандартизацию процессов, то стартап действует в условиях высокой неопределенности, ограниченных ресурсов и жесткого временного давления, где потеря нескольких месяцев часто равна потере рыночного окна. Статистика причин неудач подтверждает эту зависимость: среди ключевых факторов закрытия проектов регулярно называются отсутствие подтвержденного спроса, просчеты в продуктовой логике и проблемы организационного управления [1]. М. Santamessa и соавторы связывают провал не только с финансами, но и с неспособностью команды своевременно перестраивать бизнес-модель [2].

В этих условиях интерес к гибким методологиям закономерен: Agile поддерживает короткие циклы работы, оперативную коррекцию приоритетов и постоянную связь с потребителем [3; 4]. Однако популярность Agile не гарантирует результативности: многие молодые компании заимствуют отдельные процедуры Scrum или Kanban формально, не связывая их с экономикой продукта и зрелостью команды [5]. Поэтому исследовательский фокус должен смещаться с абстрактного подтверждения пользы Agile на определение условий, при которых конкретный гибкий инструмент действительно улучшает управленческое

качество стартапа.

Управленческую результативность стартапа нельзя оценивать лишь соблюдением бюджета и плана. На ранней стадии более значимы иные показатели: скорость проверки гипотез, стоимость изменения решения, прозрачность координации в малой перегруженной команде, качество обратной связи с рынком и способность поддерживать рабочий ритм без чрезмерной бюрократизации. Именно через эти параметры следует оценивать пригодность гибких методологий для молодой компании.

Наиболее близок к логике стартапа подход Lean Startup, ориентированный на предпринимательское обучение. Э. Рис рассматривает развитие проекта через цикл «создать — измерить — научиться», где ценность создаёт не объем выполненной работы, а скорость получения подтвержденного знания о рынке [8]. В сочетании с определением С. Бланка — стартап как «временная организация, созданная для поиска повторяемой и масштабируемой бизнес-модели» [9, с. 19] — отсюда следует, что на раннем этапе управленческая система должна быть подчинена не процессной дисциплине, а скорости верификации гипотез. Поэтому Lean Startup особенно полезен на стадии pre-seed: его ценность — в снижении стоимости ошибки и в отказе от функциональности, не подтвержденной спросом.

Kanban решает смежную задачу: если Lean Startup помогает определить, что проверять, то Kanban делает видимым поток работы. Для стартапа это принципиально, поскольку небольшая команда совмещает разработку, маркетинг, продажи и операционные задачи, а скрытые задержки и перегрузка становятся источником потерь. Подход D. J. Anderson показывает, что визуализация задач и ограничение незавершенной работы повышают управляемость без жесткой реорганизации [7]. Экономический эффект Kanban — в уменьшении времени прохождения задачи и ясном распределении приоритетов; особенно он полезен на стадии seed, когда продуктовая гипотеза частично подтверждена, но команда не готова к тяжелой процессной структуре.

Scrum строится вокруг ритма коллективной поставки результата и полезен,

когда стартап выходит из первичного поиска и нуждается в устойчивой координации более сложной команды. Короткие спринты, фиксация ближайшей цели, регулярные обзоры и ретроспективы делают управленческие решения прозрачнее, а расхождение плана с фактом — заметнее [6]. Исследования показывают, что регулярная обратная связь и итеративность повышают качество взаимодействия, если у команды уже есть минимальная ролевая определенность [11; 14]. В то же время преждевременное внедрение Scrum даёт обратный эффект: команда тратит время на ритуалы без роста управляемости.

Российская предпринимательская среда вносит в применение Agile дополнительную специфику. Стартапы развиваются при ограниченном доступе к капиталу, высокой чувствительности к кассовым разрывам и необходимости совмещать рост продукта с поиском внешней поддержки, что повышает значимость инструментов, быстро отделяющих перспективные направления от затратных. Нередко доминирует фигура основателя, что ускоряет решения на раннем этапе, но затем превращается в фактор торможения масштабирования; поэтому гибкая методология работает только при перераспределении ответственности и росте самостоятельности команды. Дополнительную сложность создает кадровая неоднородность — совмещение сильных специалистов, новичков и внешних исполнителей, — и это повышает ценность прозрачности задач и краткости управленческого цикла [10; 15; 16].

Важно и то, что гибкость не равна отсутствию дисциплины: инвесторы и грантодатели ожидают от проекта не только скорости, но и управленческой объяснимости. Эффективное применение Agile требует опоры на измеримые показатели — скорость проверки гипотез, время вывода MVP, длительность прохождения задачи, долю завершённых приоритетов, показатели удержания клиентов [13]. Привязка к метрикам превращает Agile из модной идеологии в экономически значимый инструмент управления, особенно критичный там, где стоимость ошибки высока, а запас времени на коррекцию ограничен [17].

Практическая результативность гибких методологий в стартапе носит стадийный характер: на этапе поиска ценностного предложения рационален Lean

Startup, на этапе роста операционной плотности — Kanban, при расширении команды и усложнении координации — Scrum. Поэтому для российских стартапов оптимальна не ориентация на одну универсальную методологию, а последовательное и осмысленное сочетание подходов. Такая модель уменьшает неопределенность, повышает прозрачность управленческих решений и рациональнее использует ограниченные ресурсы — в этом и состоит основной экономический смысл Agile для молодой предпринимательской организации.

Список литературы

1. CB Insights. The Top 12 Reasons Startups Fail [Электронный ресурс]. 2021. URL: <https://www.cbinsights.com/research/startup-failure-reasons-top/> (дата обращения: 19.04.2026).
2. Cantamessa M., Gatteschi V., Perboli G., Rosano M. Startups' Roads to Failure / Sustainability. 2018. Vol. 10. № 7. Art. 2346.
3. Nerur S., Mahapatra R., Mangalaraj G. Challenges of Migrating to Agile Methodologies / Communications of the ACM. 2005. Vol. 48. № 5. P. 72-78.
4. Beck K., Beedle M., van Bennekum A. et al. Manifesto for Agile Software Development [Электронный ресурс]. 2001. URL: <https://agilemanifesto.org/> (дата обращения: 19.04.2026).
5. Digital.ai. 16th Annual State of Agile Report. 2022. 20 p.
6. Schwaber K., Sutherland J. The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game. 2020. 14 p.
7. Anderson D. J. Kanban: Successful Evolutionary Change for Your Technology Business. Sequim: Blue Hole Press, 2010. 278 p.
8. Ries E. The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses. New York: Crown Business, 2011. 336 p.
9. Blank S. The Four Steps to the Epiphany: Successful Strategies for Products that Win. 2nd ed. Pescadero: K&S Ranch, 2013. 370 p.
10. Паттабираман К. Управление стартапами: как руководить компанией в

условиях неопределенности / Менеджмент в России и за рубежом. 2019. № 3. С. 45-52.

11. Dingsøyr T., Nerur S., Balijepally V., Moe N. B. A Decade of Agile Methodologies: Towards Explaining Agile Software Development / Journal of Systems and Software. 2012. Vol. 85. № 6. P. 1213-1221.

12. Conboy K. Agility from First Principles: Reconstructing the Concept of Agility in Information Systems Development / Information Systems Research. 2009. Vol. 20. № 3. P. 329-354.

13. Reichheld F. The One Number You Need to Grow / Harvard Business Review. 2003. Vol. 81. № 12. P. 46-54.

14. Sutherland J. Scrum: The Art of Doing Twice the Work in Half the Time. New York: Crown Business, 2014. 256 p.

15. Rigby D. K., Sutherland J., Noble A. Agile at Scale / Harvard Business Review. 2018. Vol. 96. № 3. P. 88-96.

16. Startup Genome. The Global Startup Ecosystem Report 2022. San Francisco, 2022. 290 p.

17. Мурасова И. Р., Абрамова О. Ф. Особенности применения Agile-методологий в малых предприятиях / Молодой ученый. 2020. № 18 (308). С. 107-110.

УДК 338.43

**ЗАРУБЕЖНЫЙ ОПЫТ АГРАРНОЙ ПОЛИТИКИ В УСЛОВИЯХ
ЦИФРОВИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА****Самыкин Иван Витальевич**

аспирант

Научный руководитель: Малолетко Александр Николаевич,

д.э.н., профессор

АНО ВО Центросоюза Российской Федерации «Российский университет
кооперации», город Мытищи

***Аннотация.** В статье рассматривается трансформация аграрной политики зарубежных стран под влиянием цифровизации сельского хозяйства. Показано, как распространение цифровых технологий изменяет способы организации производства, управления ресурсами и регулирования агропродовольственных цепочек, требуя адаптации институциональной архитектуры отрасли. На примере европейских стран, США, Китая, стран БРИКС рассмотрено, как цифровая повестка встраивается в базовые инструменты аграрной политики, а также на основе проведенного обзора формулируются ориентиры для российской аграрной политики в условиях активного внедрения и использования цифровых технологий в сфере сельского хозяйства.*

***Ключевые слова:** аграрная политика, цифровизация сельского хозяйства, зарубежный опыт, государственная поддержка, цифровая инфраструктуры, продовольственная безопасность, сельские территории*

***Keywords:** agricultural policy, digitalization of agriculture, foreign experience, state support, digital infrastructure, food security, rural areas*

Цифровизация сельского хозяйства в последние годы становится одним из ключевых факторов трансформации аграрного сектора во многих странах мира.

Распространение цифровых технологий, платформенных решений, искусственного интеллекта и накопления массива данных приводит к изменению парадигм способов организации производства, управления ресурсами и взаимодействия участников агропродовольственных цепочек. Эти изменения затрагивают не только технологическую, но и институциональную архитектуру сельского хозяйства, требуя адаптации государственной отраслевой политики к новым условиям.

Для зарубежных стран цифровая трансформация аграрного сектора становится инструментом решения сразу нескольких стратегических задач: обеспечения продовольственной безопасности, повышения устойчивости и экологичности производства, расширения участия в международной торговле и повышения конкурентоспособности национальных производителей. В документах Европейского союза, ФАО ООН и национальных стратегиях развитых и развивающихся стран цифровые технологии рассматриваются как необходимое условие переходу к так называемому «умному» и устойчивому сельскому хозяйству, позволяющему более эффективно использовать природные, организационные и финансовые ресурсы, снижать уязвимость к природно-климатическим и рыночным шокам. В то же время цифровизация ставит перед аграрной политикой новые вызовы. Возникает необходимость развития соответствующей цифровой инфраструктуры и устранения цифрового неравенства между территориями и категориями хозяйств, требует выработка подходов к регулированию аграрных данных и цифровых платформ, включая вопросы доступа, совместимости данных, защиты конфиденциальности и кибербезопасности. Меняется также логика государственной поддержки – появляются практики поддержки и программы стимулирования внедрения цифровых решений.

Цель данной статьи – анализ того, как аграрная политика зарубежных стран адаптируется к условиям цифровизации. Рассматриваются примеры Европейского союза, США, Китая и других стран, для которых цифровизация аграрного сектора закреплена в стратегических документах.

Современная цифровизация сельского хозяйства описывается через

концепцию «Agriculture 4.0», которая предполагает интеграцию в сельскохозяйственное производство технологий Индустрии 4.0 – искусственного интеллекта, анализа больших данных, интернета вещей и других современных технологий [1, с.85]. Акцент смещается с отдельных технических новшеств на сквозное использование данных по всей цепочке создания стоимости. Это расширяет предмет аграрной политики, так как мимо поддержки производства и доходов фермеров, она учитывает темпы и структуру технологической модернизации, компетенции работников отрасли и характер конкуренции на рынках цифровых решений. Ключевым ресурсом современной аграрной политики становятся данные о землях, почвах, поголовье, посевах, использовании ресурсов, движении продукции и участии хозяйств в мерах поддержки, поэтому цифровизация позволяет агрегировать и анализировать такие данные, а значит точнее оценивать состояние отрасли, таргетировать поддержку и корректировать ее параметры в ответ на изменения рыночной среды. Вопрос о том, как такие возможности реализуются на практике, решается в разных странах по-разному.

Центральным инструментом аграрной политики Европейского союза выступает Общая сельскохозяйственная политика (САР), в которую активно интегрирована цифровая повестка [7], [11], [12]. Стратегические планы САР государств-членов союза включают разделы по цифровой трансформации аграрного сектора, сельских территорий, увязывают меры поддержки с развитием цифровых сервисов, цифровых компетенций, развитие инфраструктуры и оборудования. Для финансирования цифровых проектов используются не только средства национальных бюджетов, но и целый ряд общеевропейских инструментов: программа «Цифровая Европа» (Digital Europe Programme), рамочная программа «Горизонт Европа» (Horizont Europe), фонд «Соединяя Европу», Европейский фонд регионального развития, позволяющие поддерживать цифровую инфраструктуру отрасли, исследования и внедрение технологий сельскохозяйственными производителями.

Европейская комиссия формулирует цели постреформенной САР с акцентом на преодоление цифрового разрыва в сельской местности и усилении

синергии между аграрной цифровой и региональной политикой [13]. Параллельно в рамках данной политики реализуются проекты по поддержке малых и средних хозяйств в 15 странах Европейского союза, ориентированный на доступные решения для небольших ферм и разработку законодательные инициативы в их интересах. В результате можно сделать вывод, что европейская модель сочетает прямую финансовую поддержку цифровизации, регуляторные инициативы и целевые проекты под отдельные категории хозяйств.

Значимую роль в развитии цифровизации сельских территорий Европы и Центральной Азии играет инициатива «цифровых деревень», запущенная ФАО ООН в 2021 году. Ее целью является превращение сельских территорий в цифровые хабы через совместное с местными жителями проектирование решений, развитие компетенций и опору на локальные ресурсы [5]. Инициатива охватывает Албанию, Азербайджан, Боснию и Герцеговину, Турцию, Узбекистан и другие страны.

В США поддержка цифровизации сельского хозяйства ориентирована на стимулирование рыночного внедрения технологий точного земледелия и цифровых сервисов. По данным службы экономических исследований Министерства сельского хозяйства США, карты урожайности, почвенные карты и система точного земледелия, применяются на 5–25 % от общей площади посевов озимой пшеницы, хлопка, сорго и риса в США, а автоматизированные системы управления используются более чем на 50 % площадей, засеянных кукурузой, хлопком, рисом, сорго, соей и озимой пшеницей [9].

Одновременно находится в развитии законодательный контур поддержки. Законопроект Promoting Precision Agriculture Act, который предложили принять в 2025 году, предполагает разработку добровольных отраслевых стандартов, обеспечение интероперабельности цифровых решений и усиление кибербезопасности аграрных данных через скоординированную работу USDA, NIST (Национального института стандартов и технологий) и FCC (Федеральной комиссии связи) [14].

Цифровизация сельского хозяйства встроена в базовый инструмент

аграрной политики – пятилетний Закон о сельском хозяйстве (Farm Bill), который объединяет меры поддержки доходов, страхования, кредитования развития сельских территорий и охраны природных ресурсов [10]. В рамках данного закона на 2026 год точное земледелие закрепляется официально, характеризуется перечнем поддерживаемых технологий, а государственная поддержка их внедрения интегрируется в природоохранные программы Министерства сельского хозяйства США (фермерам, применяющим цифровые решения в составе экологических практик, предполагается возмещать 90% затрат). Соответственно, цифровые технологии США в сельском хозяйстве финансируются не отдельными пакетами мер, а через прямые каналы стратегической государственной поддержки. Параллельно государство инвестирует в цифровую инфраструктуру сельских территорий. Базовой программой выступает ReConnect Loan and Grant Program, через которую на строительство и модернизацию сетей широкополосного доступа в сельской местности.

В Китае комплексная модель государственной стратегии цифрового сельского хозяйства закреплена в ежегодных документах ЦК КПК и Госсовета КНР. «Документ №1» от 2026 года открывает 15-летний цикл, делает акцент на ускорении прорывов в ключевых технологиях, развития семеноводства и биологической селекции, а также расширению применения искусственного интеллекта, дронов, интернета вещей, робототехники и биопроизводства [4]. Цифровизация в результате рассматривается как главный фактор повышения производительности и продовольственной безопасности в условиях ограниченности трудовых и природных ресурсов.

Особый интерес представляет Инициатива КНР «Цифровая деревня», о начале которой Центральное правительство Китая объявило в начале 2020 года. Хорошим примером реализации является бренд Lishui Shangeng в провинции Чжэцзян. Бренд объединяет 977 компаний, сельскохозяйственных кооперативов и семейных ферм, которые занимаются производством продукции в девяти основных отраслях, включая съедобные грибы, чай, фрукты, овощи, традиционную китайскую медицину, домашний скот, масло камелии, побеги бамбука и

рыбалку. Lishui Shangeng имеет систему стандартов сертификации и систему управления прослеживаемостью. Фирменная фермерская продукция упаковывается с QR-кодом, который содержит всю информацию о продукции, от производственной зоны до логистических деталей [2, с. 90].

Цифровая трансформация аграрного сектора Китая также связана не только с экономическими перспективами, но и с возможностью роста экологизации производственных процессов, с формированием «зеленой» экономики, что очень актуально для КНР. С 2015 года Китай реализует различные стратегии и меры по поддержке «зеленого», устойчивого развития сельского хозяйства, обеспечивая прочную институциональную поддержку. Несмотря на эти усилия, «зеленое» развитие сельского хозяйства во многих провинциях остается недостаточным, со значительными региональными диспропорциями, которые требуют разрешения конфликта между сельскохозяйственным развитием и ограниченностью ресурсов, в чем как раз и способна помочь цифровизация.

В Бразилии цифровизация сельского хозяйства выстраивается вокруг государственной научно-технической инфраструктуры – Бразильской корпорации сельскохозяйственных исследований Embrapa, объединяющей 46 децентрализованных научных центров и сеть государственных, университетских и частных организаций. Цифровые сервисы и инструменты управления данными встраиваются в Отраслевой план адаптации к изменению климата и низкоуглеродной экономики АПК, действующей до 2030 года [8], который объединяет меры поддержки производителей, применяющих интегрированные системы «растениеводство-животноводство-лес» (iLF), цифровой мониторинг пастбищ и систем учета выбросов и продуктивности. Финансирование таких практик осуществляется преимущественно через льготное кредитование в рамках плана адаптации и исследовательских программ MAPA и Embrapa.

В Индии в сентябре 2024 года Союзным кабинетом утверждена программа Digital Agriculture Mission с общим финансированием 2 817 кроров рупий, включая 1940 кроров из центрального бюджета. Программа строится вокруг цифровой публичной инфраструктуры для сельского хозяйства, включающей Agri

Stack (реестр фермеров, реестр посевов и георегистр деревень), систему поддержки аграрных решений Krishi Decision Support System и карты плодородия почв [6], что позволяет увязывать выдачу кредитов, страхования и субсидий с верифицированными данными о хозяйствах. Цифровые механизмы встроены в программу субсидий, в рамках которых малые фермеры получают 55% субсидий с дополнительными региональными доплатами, тем самым цифровизация становится каналом адресной поддержки.

В Казахстане с 2016-2018 годов работает цифровая экосистема Qoldau, через которую оцифровано 100 млн. гектаров сельхозземель (90%), зарегистрировано свыше 260 тыс. пользователей и распределяется свыше 600 млн. долл. США субсидий [3].

В результате зарубежную практику цифровизации и государственного регулирования можно систематизировать следующим образом (таблица 1).

Таблица 1 - Зарубежные подходы к аграрной политике в условиях цифровизации

Страна	Повестка цифровизации в аграрную политику	Основной акцент инструментов
Европейский союз	Цифровые задачи внедрены в стратегические планы CAP и политики развития сельских территорий	Многоуровневое финансирование, поддержка малого и среднего бизнеса, снижение цифрового неравенства
США	Аспект развития цифровых технологий интегрирован в Закон о сельском хозяйстве, программы USDA	Субсидирование точного земледелия, развитие инфраструктуры, добровольные стандарты данных
Китай	Цифровое сельское хозяйство – часть национальной стратегии	Масштабные государственные инвестиции, связка цифровизации с продовольственной повесткой и повесткой в области устойчивого развития, значимая роль крупных платформ
Бразилия/Индия	Цифровизация встроена в климатические и отраслевые программы	Увязка субсидий и кредитов с цифровыми реестрами и мониторингом, ставка на развитую цифровую инфраструктуру
Казахстан	Создание национальных цифровых платформ и участие в инициативах ФАО ООН	Использование платформ, снижение цифрового неравенства территорий и типов хозяйств

Источник: составлено автором на основании проведенного исследования

Таким образом, зарубежный опыт показывает, что цифровизация

эффективна тогда, когда она реализуется не как отдельный проект, а когда она встроена в базовые инструменты аграрной политики. Кроме того, все рассмотренные страны сочетают инфраструктурные инвестиции, прямую поддержку цифровых технологий и регулирование данных.

Для российской аграрной политики ключевой урок зарубежного опыта состоит в том, что цифровизация должна рассматриваться как сквозной элемент функционирования сельскохозяйственной отрасли и ее институционального регулирования. Это означает необходимость увязки развития государственных информационных систем, Единой цифровой платформы АПК с целями продовольственной безопасности, устойчивости, экспортной политики и политики по развитию сельскохозяйственных территорий, а также четкого отражения требований по цифровым аспектам в критериях доступа к поддержке, порядке отчетности и мониторинга результатов.

Вторым важным выводом для российской практики является необходимость между стимулированием передовых цифровых решений и снижением цифрового неравенства. Зарубежные кейсы показывают, что инвестиции в сельскую связь и цифровые компетенции, специальные меры для малых форм хозяйствования являются обязательным условием того, чтобы цифровые требования не превращались в барьер доступа к поддержке. Для России это означает приоритизацию проектов, одновременно расширяющих охват цифровой инфраструктурой и упрощающих для хозяйств вход в государственный цифровой контур.

В совокупности проведенный обзор зарубежного опыта показывает, что цифровизация уже стала неотъемлемой частью аграрной политики ряда стран и используется как инструмент повышения производительности, устойчивости и конкурентоспособности сельского хозяйства. При этом институциональные конфигурации могут различаться. Для России, находящейся на этапе формирования единого цифрового контура аграрного сектора, важно не просто копировать отдельные решения, сколько учесть принципиальные элементы успешных моделей – стратегическое внедрение цифровизации в аграрную политику, сочетание масштабных инвестиций с адресной поддержкой хозяйств и создание

предсказуемого режима работы с сельскохозяйственными данными. От того, насколько последовательно и качество эти и другие меры будут реализованы, зависит, станет ли цифровизация реальным ресурсом развития аграрного сектора или останется перечнем разрозненных цифровых проектов.

Список литературы

1. Романова Ю. А., Левина Е. В. «Agriculture 4.0» – проект будущего или платформа ответа на большие вызовы и угрозы национальной безопасности / Проблемы рыночной экономики. – 2020. – № 3. – С. 84-94.

2. Саушева О. С. Цифровизация сельского хозяйства как фактор обеспечения продовольственной безопасности: опыт стран БРИКС. Фундаментальные исследования. 2024. - № 12. – С. 89-93.

3. Цифровое сельское хозяйство Казахстана: реалии, перспективы, возможности. DKN, 2022. URL: <https://dknews.kz/ru/ekonomika/242842-cifrovoe-selskoe-hozyaystvo-kazahstana-realii> (Дата обращения 19.04.2026).

4. China's no. 1 central document. New Direction of Rural Development and Food Security. Orga, 2026. URL: <https://orcasia.org/article/1605/chinas-no-1-central-document> (Дата обращения 19.04.2026).

5. Digital Villages Initiative in Europe and Central Asia. FAO. URL: <https://www.fao.org/digital-villages-initiative/europe/en> (Дата обращения 18.04.2026).

6. Digital Agriculture Mission: Tech for Transforming Farmers' Lives. Ministry of Agriculture & Farmers Welfare India? 2024. URL: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2051719®=3&lang=2> (Дата обращения 19.04.2026).

7. Digitalisation of agriculture and rural areas in the EU. European Commission. URL: https://agriculture.ec.europa.eu/overview-vision-agriculture-food/digitalisation_en (Дата обращения 18.04.2026).

8. Plan for adaptation and low carbon emission in agriculture. MAPA, 2021. URL: <https://www.gov.br/agricultura/pt-br/assuntos/sustentabilidade/planoabc-abc-mais/publicacoes/abc-english.pdf> (Дата обращения 19.04.2026).

9. Precision Agriculture in the Digital Era: Recent Adoption on U.S. Farms. USDA. 2023. URL: <https://www.ers.usda.gov/publications/pub-details?pubid=105893> (Дата обращения 19.04.2026).

10. RELEASE: 2026 House Farm Bill Advances Innovation Priorities, but Senate Action Still Needed. Breakthrough, 2026. URL: <https://thebreakthrough.org/press/release-2026-house-farm-bill-advances-innovation-priorities-but-senate-action-still-needed> (Дата обращения 18.04.2026).

11. The Digital Europe Programme. European Commission. URL: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme> (Дата обращения 19.04.2026).

12. The common agricultural policy at a glance. European Commission. URL: https://agriculture.ec.europa.eu/common-agricultural-policy/cap-overview/cap-glance_en (Дата обращения 19.04.2026).

13. The CAP post-2027 in the next EU budget. European Commission. URL: https://agriculture.ec.europa.eu/common-agricultural-policy/cap-post-2027-next-eu-budget_en (Дата обращения 19.04.2026).

14. U.S. senators reintroduce bill to boost precision agriculture. Future Farming, 2025. URL: <https://www.futurefarming.com/smart-farming/u-s-senators-reintroduce-bill-to-boost-precision-agriculture/> (Дата обращения 18.04.2026).

ЮРИДИЧЕСКИЕ НАУКИ

УДК 340

НОВЫЕ ПОДХОДЫ К ОХРАНЕ НЕДВИЖИМОГО ИМУЩЕСТВА В УСЛОВИЯХ РОСТА КИБЕРМОШЕННИЧЕСТВА И РЕЙДЕРСТВА В РОССИИ

Малыгина Ия Максимовна

магистрант

Научный руководитель: Епифанова Татьяна Владимировна,

д.э.н., к.ю.н., доцент, профессор

РГЭУ (РИНХ) «Ростовский государственный экономический университет»,
город Ростов-на-Дону

***Аннотация.** Появление новых видов мошенничества, использующих цифровые технологии и психологическое давление, вместе с классическим захватом недвижимости заставляет собственников искать новые пути защиты своего имущества. Сегодняшняя опасность связана главным образом с обманом владельцев и несовершенством учёта прав собственности. Для борьбы с такими угрозами разработаны свежие стратегии, включающие применение цифровых решений, страховки и юридических методов, нацеленных на профилактику нарушения прав, а не на устранение последствий после потери имущества.*

The emergence of new types of fraud using digital technologies and psychological pressure, along with the classic seizure of real estate, forces owners to look for new ways to protect their property. Today's danger is mainly related to the deception of owners and imperfect accounting of property rights. To combat such threats, fresh strategies have been developed, including the use of digital solutions, insurance and legal methods aimed at preventing violations of rights, rather than eliminating the consequences after the loss of property.

Ключевые слова: недвижимое имущество, рейдерство, «эффект

Долиной», страхование, методы, мошенники

Keywords: *real estate, raiding, «Valley effect», insurance, methods, fraudsters*

Охрана недвижимого имущества сегодня сталкивается с качественно новыми рисками, которые сложно устранить стандартными юридическими процедурами.

Все больше в современном мире сталкиваются с новыми не изученными, изощренными схемами мошенничества: преступники используют методы социальной инженерии. При схеме с «безопасным счетом» злоумышленники звонят гражданам, представляясь сотрудниками правоохранительных органов, государственных учреждений или финансовых организаций. Они предупреждают о сомнительных банковских операциях и убеждают перевести деньги на специальный счет или передать наличные курьеру, иногда угрожая уголовной ответственностью за различные нарушения.

Используются нейросети для генерации голосов, а для вывода средств привлекаются «биодропы» — лица, также находящиеся под влиянием мошенников.

По данным МВД в январе — июле 2025 года было зафиксировано 425 тысяч киберпреступлений, вследствие чего россияне потеряли около 119 млрд рублей, а это на 16% больше, чем за аналогичный период предыдущего года. В Центробанке подтверждают тревожную динамику: только в 3-м квартале 2025 года злоумышленникам удалось совершить порядка 460 тысяч мошеннических операций, что превышает среднее значение предыдущих четырех кварталов на целых 51% [1].

Не стоит заблуждаться, что жертвами мошенников становятся лишь крайне доверчивые и технически неграмотные люди. Жертвой злоумышленников может стать каждый.

Сделки, совершенные под влиянием обмана, создают риски для добросовестных покупателей. Случай с певицей Ларисой Долиной («эффект Долиной») стал новым этапом данной проблемы. Признание судами таких сделок незаконными может привести к тому, что покупатель лишается и жилья, и вложенных средств, ставя под угрозу надежность рынка недвижимости. Однако Верховный

Суд РФ подчеркивает важный нюанс: ошибочное представление одной стороны относительно мотивации заключения договора не служит достаточным поводом для признания сделки недействительной, если вторая сторона действовала добросовестно [2].

Так же активно рейдеры используют передовые методы проникновения, включая использование дронов, тепловизоров, специальных инструментов и программного обеспечения для обхода традиционных охранных систем. Это обстоятельство требует постоянного обновления технических решений защиты недвижимости.

Коллизия в системе регистрации прав порождает дополнительные уязвимости, используемые рейдерами путем анализа технических ошибок либо задержек внесения сведений в ЕГРН [3]. Недостаточная координация между ведомствами и трудности, возникающие при обжаловании уже зарегистрированного права, повышают риск потери собственности законными владельцами. Эти обстоятельства подчеркивают важность внедрения эффективных мер контроля качества регистрационных процедур и повышения прозрачности процесса обработки документов органами Росреестра. Дополнительно возрастает значимость страхования рисков утраты недвижимости, связанного с подобными ситуациями, а также внедрение технологических решений, минимизирующих вероятность возникновения подобного рода угроз.

В результате возникшей ситуации была разработана система инновационных профилактических мер для защиты объектов недвижимости.

1. Одно из эффективных мер является внесение специальной отметки в ЕГРН, запрещающей проведение любых регистрационных действий без личного присутствия собственника или при наличии судебного спора. По данным Росреестра, 738 тыс. россиян запретили сделки с недвижимостью без их личного участия в первом полугодии 2025-го. Это в два раза больше, чем за тот же период 2024-го [4].

2. Развитие онлайн-сервисов Росреестра позволяет собственникам оперативно отслеживать все юридически значимые действия с их имуществом.

Созданный Росреестром виртуальный ассистент-регистратор «Ева» обеспечивает автоматизированный приём документации в многофункциональных центрах предоставления услуг (МФЦ) и частично автоматизирует процесс обработки этих документов внутри ведомства. По словам ведомства использование цифрового помощника — регистратора «Ева» — позволило сократить время приема документов при регистрации прав собственности на недвижимость с 25 до 5 минут [5].

3. Титульное страхование представляет собой страховку права владения недвижимым имуществом. Если спустя некоторое время окажется, что продавец не имел законных оснований на продажу квартиры (например, объявятся незаявленные наследники или обнаружатся поддельные документы), страховая организация компенсирует владельцу полную стоимость жилья.

Данный вид страхования относится к числу дорогостоящих продуктов для частных лиц. Цена страхового полиса варьируется от 0,2% до 0,5% от оценочной стоимости недвижимости. Например, за жильё стоимостью 10 миллионов рублей придётся единовременно заплатить около 20 тысяч до 50 тысяч рублей. Срок действия страховки ограничен и обычно составляет три года, хотя возможно заключение договоров на более длительный период, однако это увеличит общую стоимость услуги [6].

4. Период «охлаждения» для средств

Начиная с 2025 года, в России функционирует отдельный механизм под названием «период охлаждения». Данный механизм устанавливает временную паузу перед выдачей кредитов или переводом средств, направляя усилия на снижение рисков мошенничества при выполнении банковских транзакций.

По официальным сведениям, начиная с 1 сентября 2025 года, введен «период охлаждения», нацеленный на защиту россиян от мошеннических действий. Банковские организации теперь обязаны соблюдать интервал от 4 до 48 часов после одобрения кредитной заявки, прежде чем предоставить заемщику денежные средства. Продолжительность этого интервала определяется размером предоставляемого займа [7].

5. Защита добросовестного приобретателя

С целью защиты добропорядочных субъектов рынка недвижимости и стабилизации условий гражданского оборота вторичной жилой недвижимости Государственная Дума разработала дорожную карту по решению этой проблемы.

Согласно нынешнему российскому законодательству, добросовестный покупатель недвижимости вправе рассчитывать на возмещение ущерба от государства в определенных обстоятельствах, предусмотренных статьей 68.1 Федерального закона «О государственной регистрации недвижимости». Условия выплаты такой компенсации изложены в статье 302 Гражданского кодекса РФ. Тем не менее, существующие положения не распространяются на ситуации, когда собственник продал жилье под внешним давлением или обманом. В разрабатываемой дорожной карте предложено включить подобные случаи в список ситуаций, подлежащих защите посредством выплат государственной компенсации [8].

В Госдуме обсудили доработку закона о компенсации за утраченное жилье жертвам мошенников. На данный момент изменений не наблюдается.

В связи с этим есть надежда, что пленум ВС вынесет определение с разъяснениями по реализации решений судов о вопросе недвижимости, а именно что квартира возвращается владельцу исключительно при условии возврата денег) [9].

6. Так как основная масса сделок с недвижимостью, включая случаи мошенничества, проходит через посредническое участие агентов по недвижимости, именно они способны первыми заметить признаки неблагонадежности. Поэтому одним из пунктов разработанной карты предусмотрено тесное сотрудничество риелторского сообщества с представителями Министерства внутренних дел. [10]. Предполагается, что каждая региональная структура МВД должна назначить конкретного сотрудника, который будет доступен для обращений риелторов при возникновении подозрений. Данный представитель обязан быстро среагировать на поступившую информацию и, если потребуется, провести проверку фактов в течение суток.

7. Обычно потенциальные жертвы мошенничества, готовящие продажу

жилья, не ставят в известность своих родных и близких, несмотря на то, что именно они могли бы повлиять на решение собственника отказаться от подобной операции. В целях сокращения числа таких сделок Росреестру рекомендовано рассмотреть внедрение нового инструмента — механизма двойной верификации. Эта мера подразумевает самостоятельное установление владельцем недвижимости автоматической блокировки на изменение статуса права собственности без подтверждения от доверенного лица, выбранного самим собственником. Таким образом, снятие установленной блокировки станет возможным лишь после подтверждения вторым лицом. Что касается граждан, относящихся к группе повышенного риска стать жертвами телефонных мошенников, предлагается дополнительно проанализировать целесообразность установки автоматического оповещения ближайших родственников при осуществлении юридических действий с недвижимостью. Такое уведомление могло бы осуществляться через специализированный раздел «Близкие» на портале «Госуслуги» [11].

Подводя итоги, становится ясно одно: традиционные способы защиты имущества безнадежно устарели. Если раньше надежные замки и сигнализации внушали уверенность в сохранности дома, то сегодня это лишь иллюзия безопасности. Мир изменился коренным образом, и главные угрозы переместились в цифровое пространство.

Сегодня собственность крадут не физически, а виртуально, используя современные технологии и лазейки в законах. Преступники больше не вооружены ломом и отвертками — теперь они орудуют компьютером и доступом к вашим данным. Именно поэтому простого забора и камер наблюдения недостаточно. Необходимо заботиться о цифровой безопасности своей недвижимости, контролировать состояние документов и активно использовать меры предосторожности, предложенные государством.

Современному владельцу жилья важно понимать: залог надежной защиты — владение актуальной информацией и контроль над всеми юридическими аспектами владения недвижимостью. Современные технологии одновременно облегчают нашу жизнь и создают риски для преступников. Основная цель

собственников должна заключаться не столько в физической охране жилища, сколько в предотвращении цифрового проникновения злоумышленников к своим правам на имущество.

Список литературы

1. Какие схемы мошенничества будут распространены в 2026 году и как не потерять свои деньги. — Текст: электронный /Финансовый маркетплейс: [сайт]. — URL: <https://www.banki.ru/news/daytheme/?id=11020662>) (дата обращения: 13.04.2026).

2. ВС РФ признал действительной сделку по продаже квартиры, совершенную под влиянием мошенников. — Текст: электронный / КонсультантПлюс: [сайт]. — URL: <https://www.consultant.ru/legalnews/30348> (дата обращения: 13.04.2026).

3. Цалкосов А. Б., Цаликова М. Б. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРАВ НА НЕДВИЖИМОЕ ИМУЩЕСТВО / Научный Лидер. 2025. №25 (226). URL: <https://scilead.ru/article/9407-aktualnie-problemi-gosudarstvennoj-registrats>

4. Число запретов на сделки с жильем без личного участия в России удвоилось. — Текст: электронный / ДомКлик: [сайт]. — URL: <https://blog.domclick.ru/novosti/post/chislo-zapretov-na-sdelki-s-zhilem-bez-lichnogo-uchastiya-v-rossii-udvoilos> (дата обращения: 13.04.2026).

5. Росреестр расширяет применение ИИ-сервисов. Текст: электронный/Коммерсант: [сайт]. URL: <https://www.kommersant.ru/doc/7562935> (дата обращения: 13.04.2026).

6. Титульное страхование недвижимости: что это, как работает и когда нужно. Текст: электронный/Российская газета: [сайт]. —URL: <https://rg.ru/2025/09/22/titulnoe-strahovanie-nedvizhimosti-chto-eto-kak-rabotaet-i-kogda-nuzhno.html> (дата обращения: 13.04.2026).

7. Новый закон о периоде охлаждения с 1 сентября 2025: что изменилось для вас. Текст: электронный/bankiros:[сайт].—URL: <https://bankiros.ru/wiki/term/>

`как-rabotaet-period-ohlazdenia-v-2025-otkaz-ot-strahovki-i-zasita-ot-mosennikov`
(дата обращения: 13.04.2026).

8. Разработана дорожная карта по защите рынка жилья от «эффекта Долиной». — Текст: электронный / РБК: [сайт]. — URL: <https://realty.rbc.ru/news/6932a1b19a79472b29a292d7?from=cory> (дата обращения: 13.04.2026).

9. В Госдуме предложили доработать закон о компенсации за утраченное жилье. — Текст: электронный / Новости: [сайт]. — URL: <https://news.mail.ru/economics/68808290/> (дата обращения: 13.04.2026).

10. «Открытый диалог» Росреестра с представителями профессиональных риелторских сообществ Российской Федерации. — Текст: электронный / Районные вести: [сайт]. — URL: <http://rayvesti22.ru/2022/12/01/otkrytyj-dialog-rosreestra-s-predstavitelyami-professionalnyx-rieltorskix-soobshhestv-rossijskoj-federacii/> (дата обращения: 13.04.2026).

11. Сервис «Близкие рядом»: что это такое, как пользоваться и стоит ли подключать в 2026 году. — Текст: электронный / Рамблер: [сайт]. — URL: https://life.rambler.ru/instructions/56039984/?utm_content=life_media&utm_medium=read_more&utm_source=corylink (дата обращения: 13.04.2026).

**«ФУНДАМЕНТАЛЬНАЯ И ПРИКЛАДНАЯ НАУКА:
НАУЧНО-МЕТОДИЧЕСКИЕ И ПРАКТИЧЕСКИЕ
АСПЕКТЫ»**

XI Международная научно-практическая конференция
Научное издание

ООО «НИЦ ЭСП» в ЮФО
(Подразделение НИЦ «Иннова»)
353445, Россия, Краснодарский край, г.-к. Анапа,
ул. Весенняя, 8, оф. 1
Тел.: 8-800-201-62-45; 8 (861) 333-44-82