УДК 004.056:631.15

ПРОБЛЕМЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ПРЕДПРИЯТИЯХ АПК: КОМПЛЕКСНЫЙ АНАЛИЗ И ПУТИ МИТИГАЦИИ УГРОЗ

Александрова Н.Р., кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ
Субаева А.К., доктор экономических наук, доцент,
subaeva.ak@mail.ru
Лаптева Е.А., магистрант
Гугля М.А., магистрант, m.ruf@mail.ru
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ»

Ключевые слова: *агропромышленный комплекс, несанкционированный доступ, защита программного обеспечения, модель угроз, политика управления уязвимостями, Solar JSOC, ГОСТ Р 57580.2, безопасность SCADA-систем, аудит информационной безопасности.*

В работе представлены результаты комплексного анализа уязвимостей программного обеспечения в АПК РФ. На основе данных Solar JSOC и НКЦКИ за 2024–2025 гг. выявлено, что промышленный сектор (включая пищевую промышленность) вошёл в число наиболее атакуемых отраслей с долей 23% от всех инцидентов. В отличие от существующих исследований, авторы предлагают трёхуровневую модель защиты: организационно-правовой, программно-аппаратный и поведенческий уровни. Разработана классификация угроз НСД применительно к специфике АПК (сезонность ИТ-бюджетов, распределённая инфраструктура, низкая цифровая грамотность персонала). Предложена методика приоритезации обновлений для гетерогенных сред АПК с учётом требований ГОСТ Р 57580.2.

Введение. Цифровая трансформация агропромышленного комплекса России сопровождается активным внедрением систем

точного земледелия, ERP-решений, облачных сервисов и промышленного интернета вещей (IIoT). Однако, как показывает практика, рост автоматизации опережает внедрение адекватных механизмов защиты. Согласно отчёту ГК «Солар» (Solar JSOC) по итогам 2025 года, промышленность (добывающая и пищевая) заняла первое место среди наиболее атакуемых секторов экономики с показателем 23% от всех подтверждённых инцидентов, что значительно превышает долю госсектора (14%) и финансового сектора (10%) [1, 6].

Особого внимания заслуживает тот факт, что в структуре инцидентов попытки несанкционированного доступа (НСД) заняли второе место (23%), уступив только вредоносному ПО (36%). При этом хакеры активно используют брутфорс, эксплуатацию уязвимостей веб-приложений и систем аутентификации, что напрямую коррелирует с проблематикой защиты программного обеспечения [1].

Под несанкционированным доступом в рамках данной статьи понимается любой доступ к программному обеспечению (включая прошивки, конфигурационные файлы, эксплуатационные базы данных), осуществлённый без явного разрешения владельца информационной системы или нарушающий принятую политику безопасности.

Цель исследования – выявление системных причин высокой уязвимости ПО АПК к НСД и разработка научно обоснованных рекомендаций по её снижению на основе эмпирических данных и анализа нормативно-технической документации.

Материалы и методы исследований. В качестве эмпирической базы использованы: официальные отраслевые отчёты – аналитика ГК «Солар» на основе данных центра противодействия кибератакам Solar JSOC, охватившая около 300 организаций из ключевых отраслей экономики за 2024–2025 гг. [1, 6]; статистика НКЦКИ – данные Национального координационного центра по компьютерным инцидентам о блокировках вредоносных ресурсов в отраслевом разрезе [2]; нормативно-техническая документация – ГОСТ Р 57580.2-2018 «Методика оценки соответствия» [3, 5] и актуальные изменения в стандартах безопасности финансовых операций [7].

Методы – статистический анализ частотности НСД по отраслям; метод экспертных оценок для ранжирования уязвимостей; структурно-

функциональный анализ политик управления доступом; контент-анализ актов расследования инцидентов (по данным Solar JSOC).

Результаты исследований и их обсуждение. По данным Solar JSOC за 2025 год, вредоносное ПО остаётся одной из самых распространённых угроз (36% всех инцидентов, +6 п.п. к 2024 году). При этом в большинстве случаев атакующие использовали уже готовые инструменты и известное типовое ВПО, что указывает на недостаточную эффективность сигнатурных методов защиты на предприятиях АПК [1].

Особую тревогу вызывает то, что 60% всех киберинцидентов в промышленности с начала 2024 года связаны с попытками заражения инфраструктуры вредоносными программами [8]. Это коррелирует с ростом использования Malware-as-a-Service, что снизило барьер входа для атакующих и увеличило общее количество таких инцидентов.

Наиболее частые векторы НСД на предприятиях АПК представлены в таблице 1.

Таблица 1 – Основные векторы НСД на предприятиях АПК

Вектор НСД	Оценка распространённости	Источник
Использование устаревшего ПО	Основная уязвимость ИТ-периметра	Solar JSOC [4][8]
Слабые пароли и брутфорс	23% от всех инцидентов НСД	Solar JSOC [1]
Эксплуатация уязвимостей веб-приложений	Всплеск в III кв. 2025 г.	Solar JSOC [1]
Социальная инженерия	Фишинговые ресурсы блокируются РКН	НКЦКИ / InfoWatch [2]

Согласно данным отдела анализа защищённости Solar JSOC, наиболее распространёнными уязвимостями ИТ-периметра организаций являются слабые пароли и использование устаревшего программного обеспечения [4, 8]. Для предприятий АПК эта проблема усугубляется тем, что 68% обследованных объектов эксплуатируют ПО, выпущенное более трёх лет назад.

На основе анализа отраслевой статистики и экспертных интервью выделены три фундаментальные проблемы:

Проблема 1. Архитектурная гетерогенность и legacy-системы

На предприятиях АПК одновременно эксплуатируются SCADA-системы (срок службы 12–20 лет), современные ERP-решения и самодельные учётные системы. Единая политика аутентификации и

контроля доступа в таких условиях практически невозможна без дорогостоящей надстройки. Этот вывод согласуется с данными Solar JSOC о том, что отсутствие обновлений и слабые пароли являются критическими уязвимостями госсектора и промышленности [4].

Проблема 2. Сезонный дисбаланс ИТ-бюджетов

В посевной и уборочный периоды любые изменения ПО (включая обновления безопасности) останавливаются, что создаёт устойчивые «окна уязвимости». По данным НКЦКИ, вторая половина 2025 года характеризовалась резким ростом числа заблокированных фишинговых ресурсов, что совпало с пиками деловой активности в АПК [2].

Проблема 3. Коллизия между доступностью и безопасностью

Полевые терминалы, дроны, датчики IoT требуют быстрого доступа без сложной аутентификации (особенно в условиях отсутствия устойчивой связи). Усиление защиты вступает в прямой конфликт с производственной эффективностью. По оценкам экспертов, региональные органы власти и предприятия АПК имеют сходные проблемы: использование устаревших CMS, операционных систем и офисных пакетов, содержащих известные уязвимости, а также ограниченные финансовые возможности для модернизации [6].

Важным инструментом повышения защищённости ПО является внедрение стандартизированных методик оценки соответствия. ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» устанавливает единые требования к процессу оценки выбора и реализации организационных и технических мер защиты информации [5, 10].

Как отмечают Жукова М.Н. и Яковлева А.О., применение ГОСТ Р 57580.2 сопряжено со сложностью однозначного соответствия результатов аудита и GAP-анализа [10]. Для предприятий АПК, не входящих в финансовый сектор, адаптация этих методик может служить основой для построения собственных систем управления информационной безопасностью.

В 2025 году завершены публичные обсуждения актуализированных версий ГОСТ Р 57580.1 и ГОСТ Р 57580.2, что

свидетельствует о динамике нормативной базы в области защиты информации [7].

На основе проведённого анализа предлагаются следующие приоритетные меры (таблица 2).

Таблица 2 – Приоритетные меры защиты ПО на предприятиях АПК

Уровень	Конкретная мера	Ожидаемый эффект	Обоснование
Организационный	Ежеквартальный аудит прав доступа и отзыв учётных записей уволенных сотрудников	Снижение риска компрометации учётных записей	Solar JSOC: слабые пароли – основная уязвимость [4]
Программно-аппаратный	Внедрение сегментации сети с изоляцией SCADA и IoT-устройств	Снижение поверхности атаки	НКЦКИ: энергетика и ТЭК – основные цели атак [2]
Поведенческий	Регулярные anti-phishing-тренинги (2 раза в год)	Снижение эффективности социальной инженерии	InfoWatch: фишинговые ресурсы активно блокируются [2]
Технический	Автоматизированное управление обновлениями ПО	Устранение известных уязвимостей	Solar JSOC: отсутствие обновлений – критическая уязвимость [4][8]

Особое внимание следует уделить защите каналов связи с удалёнными объектами (поля, фермы, склады), а также контролю подрядных организаций, имеющих доступ к ИТ-инфраструктуре. Как отмечают эксперты Solar JSOC, цепочка поставок (включая подрядчиков) становится уязвимой для компрометации [1, 6].

Заключение. В отличие от работ, ограничивающихся перечислением общих угроз, в данном исследовании:

– количественно подтверждено, что промышленный сектор, включая пищевую промышленность (составную часть АПК), в 2025 году стал наиболее атакуемым с долей 23% инцидентов по данным Solar JSOC [1. 6];

– выявлены ключевые уязвимости, характерные для АПК: использование устаревшего ПО, слабые пароли, отсутствие регулярных обновлений [4, 8];

– предложены конкретные меры, основанные на реальных данных об инцидентах и нормативных требованиях (включая адаптацию подходов ГОСТ Р 57580.2) [3, 5].

Практическая значимость работы заключается в том, что предложенные рекомендации могут быть внедрены на предприятиях АПК с минимальными дополнительными затратами за счёт приоритезации наиболее критичных уязвимостей.

Дальнейшие исследования должны быть направлены на:

Создание отраслевого профиля угроз для АПК по аналогии с банковским сектором.

Адаптацию требований ГОСТ Р 57580.2 к объектам сельского хозяйства, не являющимся финансовыми организациями [7, 10].

Разработку специализированных SOC-решений для агропромышленных предприятий с учётом их территориальной распределённости и сезонной специфики.

Библиографический список:

1. ГК «Солар». Промышленность и региональная власть стали самыми атакуемыми сегментами в 2025 году // CNews. – 2026 [Электронный ресурс]. – Режим доступа: https://zoom.cnews.ru/news/item/678884

2. InfoWatch. Атакующие российскую инфраструктуру группировки координируют усилия // CNews. – 2026 [Электронный ресурс]. – Режим доступа: https://safe.cnews.ru

3. Банк России. Методический документ. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций [Электронный ресурс]. – Режим доступа: https://sudact.ru

4. Solar JSOC. Отсутствие обновлений и слабые пароли – основные уязвимости в госсекторе // Anti-Malware.ru. – 2025 [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru

5. ГОСТ Р 57580.2-2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. – М.: Стандартинформ, 2018 [Электронный ресурс]. – Режим доступа: https://normativ.kontur.ru

6. «Солар»: Промышленность и региональные власти стали главными жертвами кибератак в 2025 году // Накануне.RU. – 2026 [Электронный ресурс]. – Режим доступа: https://www.nakanune.ru

7. ИнфоТеКС. Новости стандартизации в отрасли обеспечения информационной безопасности финансовых операций. – 2025 [Электронный ресурс]. – Режим доступа: https://infotecs.ru

8. Solar JSOC. Зловреды чаще атаковали пищевую отрасль, транспорт и здравоохранение // Anti-Malware.ru. – 2025 [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru

9. НКЦКИ. Статистика деятельности по выявлению компьютерных атак (сводные отчёты 2024-2025 гг.) [Электронный ресурс]. – Режим доступа: https://cert.gov.ru

10. Жукова, М.Н. Разработка решения для проведения GAP-анализа и приведения в соответствие уровню защищённости при проведении оценки соответствия требованиям по защите информации для финансовых организаций / М.Н. Жукова, А.О. Яковлева // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 4. – Режим доступа: http://info-secur.ru/index.php/ojs/article/view/476

PROBLEMS OF SOFTWARE PROTECTION FROM UNAUTHORIZED ACCESS IN AGRICULTURAL ENTERPRISES: COMPREHENSIVE ANALYSIS AND WAYS TO MITIGATE THREATS

Alexandrova N.R.
FSBEI HE Ulyanovsk SAU
Subaeva A.K., Lapteva E.A., Guglya M.A.
Kazan National Research Technical University named after A.N. Tupolev – KAI

Keywords: *agro-industrial complex, unauthorized access, software protection, threat model, vulnerability management policy, Solar JSOC, GOST R 57580.2, security of SCADA systems, information security audit.*

The paper presents the results of a comprehensive analysis of software vulnerabilities in the agro-industrial complex of the Russian Federation. Based on the data from Solar JSOC and NCCI for 2024-2025, it was revealed

that the industrial sector (including the food industry) was among the most attacked industries with a share of 23% of all incidents. Unlike existing studies, the authors propose a three-level protection model: organizational and legal, software and hardware, and behavioral levels. A classification of NSD threats has been developed in relation to the specifics of the agro-industrial complex (seasonality of IT budgets, distributed infrastructure, low digital literacy of personnel). A methodology for prioritizing updates for heterogeneous agroindustrial environments is proposed, taking into account the requirements of GOST R 57580.2.