**DOI 10.36622/1682-7813.2024.27.4.008**
**УДК 004.896:004.56:007.52:008.2**

# КИБЕРБЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ МОНИТОРИНГА ЛЕСНЫХ ТЕРРИТОРИЙ

**В.А. Минаев, А.С. Толпыгин, К.М. Бондарь**

В статье рассматривается вопрос применения беспилотных авиационных систем (БАС) общего назначения вблизи критически важных объектов, к которым относятся объекты оборонного комплекса, энергетики и другие. Обсуждается проблема кибербезопасности БАС, связанная с угрозами объектам критической информационной инфраструктуры. Ввиду имеющихся ограничений на полеты беспилотных летательных аппаратов (БПЛА) указанная проблема освещается в научной литературе явно недостаточно. При этом имеются пробелы в законодательном и нормативном регулировании данного вопроса. Рассматривается модельный пример применения ЬПЛА для мониторинга лесных территорий. Перечисляются элементы БАС, составляющие объект защиты, устанавливается связь с системой моделей угроз и нарушителей.

**Ключевые слова:** кибербезопасность, беспилотные летательные аппараты, беспилотные авиационные системы, искусственный интеллект, модель угроз, мониторинг лесных территорий, обнаружение пожаров.

## Введение

Мониторинг лесных территорий является одной из ключевых задач Федерального агентства лесного хозяйства (Рослесхоз).

Агентство осуществляет государственный лесной надзор – лесную охрану [1]. В рамках выполняемых функций осуществляется установление границ зон контроля, разработка планов тушения лесных пожаров, формирование федерального штаба по координации деятельности по тушению лесных пожаров и соответствующих региональных штабов. Особое внимание уделяется контролю достоверности информации о пожарной опасности в лесах, представляемой региональными лесными ведомствами.

Решение задачи своевременного (раннего) обнаружения лесных пожаров [3], формирования сухостоя и других их источников экологических катастроф с применением современных средств видеонаблюдения, машинного зрения и искусственного интеллекта является актуальной, поскольку позволяет предотвратить значительные ущербы экосистеме лесных массивов, безопасности окружающей среды и населенным пунктам, находящимся вблизи источников возгорания.

Одна из ключевых проблем в предотвращении лесных пожаров заключается в осуществлении автоматизации мониторинга обширных территорий. Важно оперативно выявлять очаги возгорания и опасные зоны, возникающие как природным путём, так и вследствие техногенных аварий, утечки опасных веществ и других факторов.

В настоящее время существует множество подходов к реализации мониторинга лесных массивов, среди которых выделяются такие методы, как установка стационарных вышек с камерами видеонаблюдения и спектральными анализаторами, дистанционное зондирование Земли с помощью спутников и авиации.

Для повышения эффективности поиска, детектирования и идентификации возгораний особую актуальность приобретает использование БПЛА и технологии искусственного интеллекта.

Основной системой мониторинга лесных массивов на предмет пожарной опасности и пожаров, осуществляющей обнаружение пожаров, наблюдение за ними и прогнозирование их развития с использованием средств дистанционного зондирования является Информационная система дистанционного мониторинга лесных пожаров Федерального агентства лесного хозяйства (ФГИС ИСДМ-Рослесхоз).

Основным источником информации в решении задач мониторинга являются спутниковые системы наблюдения.

В некоторых работах, посвящённых теме мониторинга лесов, например, [3], предлагается использовать различные технические средства и программное обеспечение, включая mesh-сети и искусственный интеллект.

Тем не менее, создание комплексного, удобного в использовании и экономически выгодного аппаратно-программного решения для предупреждения лесных пожаров в реальном времени остаётся актуальным.

**Угрозы кибербезопасности**

Одним из важных аспектов, который остается недостаточно раскрытым при разработке беспилотных авиационных систем мониторинга лесных массивов, является кибербезопасность.

В частности, в ГОСТ Р 70802-2023 не содержатся прямые требования обеспечения кибербезопасности или указания на официальные документы, устанавливающие такие требования.

Тем не менее, в нем имеются две ссылки на:

– ГОСТ 59519-2021, предполагающий только защиту от стороннего вмешательства на уровне линии управления и контроля (п. 7.1.2.2). При этом предусмотрена защита линии управления и контроля посредством кодирования с использованием ключей защиты.

– ГОСТ Р 56122-2014, рассматривающий только обеспечение надежности связи (п. 4.3.7).

Зачастую лесные массивы связаны с размещением в них объектов оборонного и оборонно-промышленного комплекса, критической инфраструктуры городов, энергетики, химической промышленности и других (далее, критически важные объекты – КВО). Несмотря на усиленные противопожарные меры, принимаемые для таких объектов, требуется дополнительные меры контроля очагов возгорания и распространения пожаров, для чего применяют беспилотные авиационные системы.

Угрозы кибербезопасности БАС связаны с угрозами объектам критической информационной инфраструктуры (КИИ). Критичными угрозами кибербезопасности в данном случае являются угрозы с потерей или перехватом управления БАС, реализация которых потенциально ведет к атакам на объекты КВО.

В действительности к БАС прямо не применяются требования Федерального закона № 187-ФЗ, как для объектов критической информационной инфраструктуры, но значимость обеспечения их кибербезопасности от этого не снижается.

В Российской Федерации существует ряд законодательных актов и документов, регулирующих использование БПЛА в целом и их эксплуатацию рядом с объектами КИИ. Вот некоторые ключевые документы:

– Федеральный закон № 149-ФЗ, регулирует отношения возникающие при обеспечении защиты информации [7];

– Указ Президента РФ № 31с касается создания системы защиты от компьютерных атак, которая может включать меры по защите БАС [8].

– Федеральный закон № 16-ФЗ регулирует вопросы обеспечения безопасности на транспорте, включая воздушные суда, в том числе беспилотные.

– Постановление Правительства РФ № 127 устанавливает правила использования БПЛА над объектами топливно-энергетического комплекса, которые могут относиться к объектам КИИ [10].

– Приказ Министерства транспорта РФ № 152 от 18 сентября 2008 г. определяет порядок использования воздушного пространства, включая зоны ограничения полетов для БПЛА.

Эти документы устанавливают рамки для безопасного использования БПЛА, особенно в зонах, где расположены объекты КИИ, требуя соблюдения строгих норм безопасности и координации действий с соответствующими органами власти. Опираясь на перечисленные нормативно-правовые акты возможно определить перечень требований информационной и кибербезопасности к БАС и построить

соответствующее дерево метрик для оценки защищенности.

Защита БАС, используемых вблизи объектов КВО, является комплексной задачей и требует:

– защиты данных: обеспечение конфиденциальности, целостности и доступности информации, передаваемой между компонентами БАС и внешними системами управления;

– управления доступом: предоставление доступа к управлению БАС только авторизованным пользователям и предотвращение возможности перехвата управления злоумышленниками;

– мониторинга и обнаружения угроз: внедрение механизмов мониторинга активности БАС и обнаружение аномалий, связанных с возможными киберугрозами;

– защиты каналов связи: использование защищенных протоколов передачи данных и средств шифрования для предотвращения перехвата или подмены команд управления;

– обновления ПО и патчей безопасности: регулярная установка обновлений ПО и устранение уязвимостей для минимизации рисков при эксплуатации.

– соответствия нормативным требованиям: соблюдение всех нормативных актов и стандартов, регулирующих использование БАС в зоне КИИ.

– резервирования отказоустойчивости: разработка резервных механизмов управления и систем защиты, обеспечивающих бесперебойную работу даже при сбоях или атаках.

– анализа рисков и моделирования сценариев: проведение регулярных оценок рисков и моделирования различных сценариев атак для своевременной адаптации мер защиты.

Для эффективного решения задачи защиты БАС от киберугроз разрабатывается и поддерживается в актуальном состоянии модель угроз и нарушителей, учитывающая все факторы угроз на жизненном цикле БАС и соответствующая система защиты. Первым приоритетом стоят угрозы, связанные с разработкой и изготовлением, а также особенностями применения БАС. По методологии, рассмотренной в [12], основу модели угроз составляют базовая и типовые модели угроз, в которых учитываются угрозы, связанные с разработкой и изготовлением, а также угрозы, связанные с типовыми элементами. Угрозы, связанные с особенностями применения БАС и угрозы, соответствующие конкретной реализации БАС – отражаются в частной модели угроз.

**Система мониторинга лесных территорий как объект защиты**

В настоящее время разрабатывается аппаратно-программная распределенная информационная система (АПРИС) мониторинга лесных территорий на основе машинного зрения, искусственного интеллекта и беспилотных летательных аппаратов.

Экспериментальный образец (ЭО) системы соответствует составу, рекомендуемому ГОСТ Р 70802-2023, включая следующие составные части (СЧ):

– БПЛА самолетного типа, дальность полета до 300 км., полезная нагрузка до 7 кг. Управление БПЛА обеспечивается из мобильной установки по радиоканалу;

– стационарные комплексы наблюдения

– быстро развертываемые вышки (опоры);

– специализированная мобильная лаборатория на базе автомобиля типа Соболь;

– мультиспектральный комплекс видеонаблюдения для стационарных и мобильных комплексов наблюдения;

– аппаратно-программный комплекс мониторинга лесных массивов, включающий распределённую систему сбора, обработки и хранения данных, сеть связи, объединяющую стационарные и мобильные комплексы наблюдения с мобильным пунктом управления;

– система связи и передачи данных на больших территориях на основе энергоэффективной электронной компонентной базы (ЭКБ);

– программное обеспечение превентивного обнаружения пожаров и других техногенных катастроф с применением машинного зрения и технологий искусственного интеллекта.

На рис. 1 показана схема организации работы и взаимодействия элементов АПРИС.

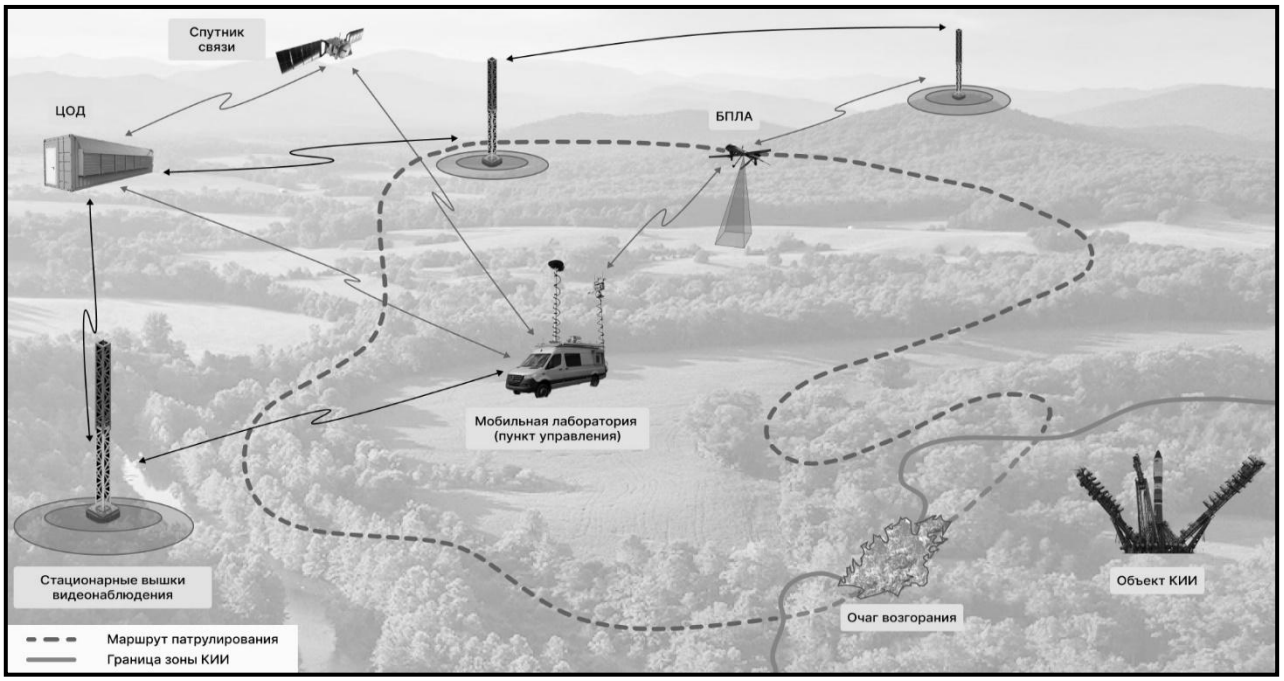


Рис. 1. Взаимодействие элементов АПРИС

Важной особенностью системы является ***киберзащищенность системы управления***, позволяющая безопасно применять БПЛА в непосредственной близости объектов КВО. Объектами защиты являются:

– система управления БПЛА;

– система связи и передачи данных;

– мультиспектральный комплекс видеонаблюдения для стационарных и мобильных комплексов наблюдения;

– аппаратно-программный комплекс мониторинга лесных массивов, включающий распределённую систему сбора, обработки и хранения данных, сеть связи, объединяющая стационарные и мобильные комплексы наблюдения с мобильным пунктом управления и ЦОД;

– программное обеспечение превентивного обнаружения пожаров и других техногенных катастроф с применением машинного зрения и искусственного интеллекта.

АПРИС предполагает следующие сценарии применения, не ограничиваясь ими:

– Сценарий 1 (основной). Мониторинг лесного массива со стационарных вышек и доразведка при помощи БПЛА.

– Сценарий 2 (ситуационный). Мониторинг лесного массива группировкой БПЛА, управляемой мобильной лабораторией.

– Сценарий 3 (комбинированный). Мониторинг лесного массива со стационарных вышек и при помощи группировки БПЛА в труднодоступных для установки вышек местах.

Местность выбирается как переменное значение по площади, может быть с перепадом высот. Площадь разделяется на области (например, квадраты по 20-60 км или по другому принципу) которые должны быть

покрыты средствами мониторинга (стационарные вышки, БПЛА) в зависимости от доступности местности, возможностей приемо-передающего оборудования и пр.

Стационарные пункты контроля ставятся на возвышенностях, по углам зон, в прямой видимости друг друга.

Вышки должны покрывать площадь мониторинга таким образом, чтобы она вся контролировалась детекторами, сенсорами, датчиками. Они могут находиться не в прямой видимости, но граница между областями видимости должна проходить не далее линии горизонта каждой.

Группировка беспилотников самолетного типа на базе электрического двигателя или двигателя внутреннего сгорания может находиться в воздухе до 4 часов.

Должны быть предусмотрены места взлёта беспилотников и места посадки для возврата БПЛА на дозаправку и техническое обслуживание с последующим выходом на маршрут патрулирования.

Угрозы кибербезопасности АПРИС могут исходить от различных внешних и внутренних нарушителей, как указано в методике оценки угроз безопасности информации ФСТЭК России от 05.02.2021.

Для определения потенциала внутреннего нарушителя, рассмотрим роли эксплуатирующего персонала:

1) *Оператор БПЛА.*

– неправомерный доступ к управлению: оператор может получить несанкционированный доступ к системе управления дроном и изменить траекторию полета, либо вывести систему из строя;

– манипуляция данными телеметрии: оператор может изменять данные о местоположении, скорости или других параметрах полета, что приведет к искажению информации о реальном состоянии системы;

– злоупотребление полномочиями: использование доступа к управлению БПЛА для выполнения личных задач, таких как слежка за объектами или шпионаж;

– неразглашение инцидентов: умышленное сокрытие сбоев или нарушений безопасности, чтобы избежать ответственности.

2) *Оператор системы мониторинга.*

– доступ к конфиденциальной информации: имея доступ к данным мониторинга, таким как маршруты полетов, состояние оборудования и другим важным сведениям, что создает риск утечки данных;

– несанкционированная передача данных: передача данных третьим, что может привести к компрометации системы;

– подмена данных: изменение или подмена данных мониторинга, что приводит к некорректным выводам и решениям;

– отказ от выполнения обязанностей: игнорирование сигналов тревоги или других важных уведомлений, что может привести к сбоям или прекращению работы системы.

3) *Водитель мобильной лаборатории* (роль может совмещена с любой из операторских):

– физический доступ к оборудованию: возможность физического вмешательства в работу оборудования, например, установка вредоносного ПО или повреждение аппаратуры;

– использование уязвимостей сети: доступ к сетям мобильной лаборатории позволяет водителю использовать слабые места в защите для проникновения в систему;

– незаконное копирование данных: копирование важной информации на внешние носители для дальнейшего использования или продажи;

– создание ложных отчетов: подделка отчетов о работе системы для сокрытия нарушений или ошибок.

4) *Инженер мобильной лаборатории:*

– изменение конфигурации системы: инженеры, обладая глубокими знаниями о системе, могут вносить изменения в конфигурацию, приводя к нарушению работы или снижению уровня защиты;

– установка закладок: внедрение скрытых программных или аппаратных средств для последующего несанкционированного доступа к системе;

– необоснованное обновление ПО: установка нелицензионного или зараженного

программного обеспечения, что может привести к взлому системы;

– предоставление привилегий: предоставление несанкционированного доступа другим сотрудникам или внешним пользователям.

5) *Инженер систем связи;*

– перехват данных в каналах связи, что позволяет получить доступ к конфиденциальной информации;

– вмешательство в трафик: изменение маршрутов передачи данных, внедрение ложных пакетов;

– атаки на инфраструктуру связи: атаки на оборудование связи, например, DDoS-атаки;

– разглашение ключей шифрования: раскрытие секретных ключей шифрования;

6) *Специалист по обработке данных.*

– искажение результатов анализа: изменение или удаление данных приводит к неверным результатам анализа;

– утечка данных: передача конфиденциальных данных третьим лицам или их публикация в открытых источниках;

– несвоевременная обработка данных: задержки в обработке критически важных данных может повлиять на принятие важнейших решений.

Учитывая область применения и функциональность мобильной лаборатории, внешние нарушители представлены следующими категориями:

1) *Террористы*.

Цели – создание хаоса, нанесение неприемлемого ущерба, привлечение внимания.

Методы воздействия:

– перехват управления БПЛА для захвата контроля и использования БПЛА в террористических актах и совершении диверсий на объектах КИИ.

2) *Хакеры.*

Цели – получение финансовой выгоды, получение доступа к конфиденциальной информации.

Методы воздействия:

– взлом системы управления БПЛА, чтобы перенаправить его или вывести из строя;

– DDoS-атака: распределенная атака против серверов аппаратно-программного комплекса мониторинга лесных массивов, включающая систему сбора, обработки и хранения данных, сеть связи, объединяющую стационарные и мобильные комплексы;

– фишинговые атаки: отправка поддельных сообщений с целью выманивания паролей или другой конфиденциальной информации;

– эксплуатация уязвимостей: использование известных или скрытых уязвимостей в программном обеспечении для получения несанкционированного доступа и искажения данных;

3) *Разведывательные службы иностранных государств.*

Цель: сбор разведданных об объектах КИИ и КВО, экономический шпионаж.

Методы воздействия:

– электронная разведка: перехват сигналов, передаваемых между элементами БАС.

– целенаправленные кибероперации: проведение многоэтапных атак с использованием сложных инструментов и методов;

– внедрение агентов для сбора информации изнутри.

Безусловно, этот перечень не является полным и приведен для того, чтобы использовать в модели угроз в ходе разработки и эксплуатации БАС.

**Обеспечение кибербезопасности АПРИС**

Для защиты от киберугроз в основу системы управления АПРИС положена цифровая платформа, описанная авторами в [14].

Встроенный комплекс средств защиты информации обеспечивает:

– управление профилями и полномочиями пользователей;

– управление доступом к информационным ресурсам, каналам передачи данных и устройствам вводы/вывода информации;

– ведение журналов регистрации системных событий;

– контроль целостности;

– контроль действий всех субъектов.

**Заключение**

В статье рассмотрены современные подходы к мониторингу лесных массивов, включая использование стационарных наблюдательных пунктов, спутниковых данных и беспилотных летательных аппаратов. Применение БПЛА признается эффективным средством для повышения оперативности и точности мониторинга, особенно в условиях труднодоступных территорий.

Отмечено, что при создании БАС упускается из виду необходимость обеспечения их информационной кибербезопасности. Применение БАС в непосредственной близости к КВО – предприятия ОПК, энергетическая инфраструктура, крупные населенные пункты, создает угрозу совершения противоправных действий посредством перехвата управления БПЛА.

Поэтому разработчики АПРИС поставили задачу создания комплексного и безопасного решения для мониторинга лесных территорий, в котором учтены не только технологические аспекты для эффективного поиска, детектирования и идентификации пожаров, но и вопросы кибербезопасности, обеспечивая тем самым надежную защиту как природных ресурсов, так и критически важных объектов, в непосредственной близости которых предполагается применение БПЛА.

**Список литературы**

1. Лесной Кодекс РФ, принят Государственной Думой РФ 8.11.2006 г., одобрен Советом Федерации 24.11.2006 г.

3. Н.Р. Вычерова Разработка системы раннего обнаружения лесных пожаров с использованием беспилотных летательных аппаратов и искусственного интеллекта / Н.Р. Вычерова, Е.А. Будевич, А.Э. Беляев // Resources and Technology. 2022. Т. 19, № 4. С. 85-101.

7. ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. № 149-ФЗ в ред. от 12.12.2023.

8. Указ Президента РФ от 15.01.2013 г. № 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

12. Минаев В.А., Толпыгин А.С. Кибербезопасность и киберустойчивость беспилотных транспортных систем // Информация и безопасность. 2024. Т. 27, № 2.- С. 177-184.

14. Минаев В.А., Толпыгин А.С. Цифровая платформа для защищенных информационно-управляющих систем беспилотного транспорта // Информация и безопасность. 2024. Т. 27, № 3. С. 309-318.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia

Московский государственный технический университет имени Н. Э. Баумана
Bauman Moscow State Technical University

Дальневосточный юридический институт МВД России
Far Eastern Law Institute of the Internal Affairs Ministry of Russia

Поступила в редакцию 3.12.24

**Информация об авторах**

**Минаев Владимир Александрович** – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

**Толпыгин Алексей Сергеевич** – канд. техн. наук, доцент кафедры «Защита информации» Московского государственного технического университета им. Н.Э. Баумана, e-mail: tolpygin@bmstu.ru

**Бондарь Константин Михайлович** – канд. техн. наук, профессор кафедры информационно-технического обеспечения ОВД Дальневосточного юридического института МВД России имени В.Ф. Шилова, e-mail: bondar_km@mail.ru

Исследование выполнено в рамках государственного задания Министерства науки и высшего образования Российской Федерации (тема № FSFN-2024-0073)

# CYBERSECURITY OF UNMANNED AERCRAFT SYSTEMS FOR MONITORING FOREST AREAS

**V.A. Minaev, A.S. Tolpygin, K.M. Bondar**

The article deals with the issue of ensuring the cybersecurity of unmanned aircraft systems (UAS) when they are used in relation to critically important objects in forest areas, which include objects of the defense complex, energy and others. Gaps in legislation and regulation of this issue are discussed. However, there are gaps in the legislative and regulatory regulation of this issue. A model example of the use of unmanned aerial vehicles (UAV) for monitoring forest areas is considered. The elements of the UAS that make up the object of protection are considered, and a connection is established with the system of threat models and violators.

**Keywords:** cybersecurity, unmanned aerial vehicles, artificial intelligence, threat model, fire monitoring.

Submitted 3.12.24

**Information about the authors**

**Vladimir A. Minaev** – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V.Ya. Kikot Moscow University of the Internal Affairs Ministry, Moscow, e-mail: m1va@yandex.ru

**Aleksey S. Tolpygin** – Cand. Sc. (Technical), Associate professor of the Information Security Department of Bauman Moscow State Technical University, Moscow, e-mail: tolpygin@bmstu.ru

**Konstantin M. Bondar** – Cand. Sc. (Technical), Professor of the Information and Technical Support Department of Internal Affairs Agencies of the Far Eastern Law Institute of the Internal Affairs Ministry of Russia named after I.F. Shilov, e-mail: bondar_km@mail.ru

The work was carried out within the framework of the state assignment of the Ministry of Science and Higher Education of the Russian Federation (topic № FSFN-2024-0073).