визуализировались. В ходе дальнейшего исследования фрагменты ПХВ-пленки изучались с помощью инфракрасной люминесценции, (адсорбционно-люминесцентный метод). В результате этого метода штрихи ПШР также не были выявлены.

Результаты проведенной работы позволяют сделать некоторые выводы. При исследовании объектов, находившихся под прямыми солнечными лучами, целесообразно применять метод микроскопического исследования и исследование в отраженных УФ-лучах. При исследовании объектов, находившихся в водной среде, наиболее эффективным методом является метод оптической микроскопии. Конечно, исследование не охватило всего спектра методов и материалов письма. Ключевым моментом нам представляется принципиальная возможность получения информации в документах, подвергшихся различным внешним факторам.

Полагаем, обозначена проблема, требующая проведения дальнейшей работы в данном направлении. В дальнейшем в рамках нового исследования планируется расширить как объем материалов письма, используемых при заполнении документов, так и комплекс методов, применяемых для получения результатов. Результаты планируется подготовить, в том числе и в иллюстративной форме, что будет некоторым ориентиром для экспертов-практиков при производстве технико-криминалистической экспертизы документов.

Минаев В.А.,

доктор технических наук
Московский Ордена почета университет МВД России им. В.Я. Кикотя

Мокшанцев А.В.,

кандидат технических наук, доцент
Академия государственной противопожарной службы МЧС России (г. Москва)

Толпыгин А.С.,

кандидат технических наук
Московский государственный технический университет им. Н.Э. Баумана

Безопасность управления беспилотным транспортом: уязвимости и угрозы

Нацеленность чрезвычайных служб Российской Федерации на опережающее противодействие неправомерному применению беспилотных авиационных систем (БАС) в сфере их ответственности привела к необходимости привлечения искусственного интеллекта (ИИ) для решения сложных оперативно-тактических, спасательных, разведывательных, следственных, криминалистических и иных задач.

Работа авторов настоящей статьи нацелена на предотвращение неправомерного применения БАС при мониторинге лесных и труднодоступных территорий, в экспертно-криминалистической деятельности, при аналитическом обеспечении раскрытия и расследования преступлений с использованием геоинформационных систем, автоматическом распознавании и маршрутизации беспилотных транспортных средств.

Как системное наполнение проведенной работы представлены материалы, раскрывающие выбор технических и нормативных решений для разработки архитектуры программного комплекса контроля и управления движением и создания цифровой защищенной платформы с целью предотвращения неправомерного применения БАС. Проанализирована достаточно объемная база международных и национальных стандартов Российской Федерации в области БАС, рассмотрены основные технические средства, системы контроля, связи и управления движением БАС, а также системы ИИ как основа безопасного управления ими.

Основные цели авторского исследования связаны с формированием систем моделей:

– киберугроз ИИ, участвующему в управлении БАС;

– киберустойчивости и управляемости флотом БАС;

– математической поддержки систем защиты информации БАС.

Всепроникающее использование БАС, к сожалению, не исключает негативные стороны данного процесса. Это касается, прежде всего, активной заинтересованности криминалитета по созданию удобных условий подготовки и совершения различных преступлений. Создание подобных условий, нередко, обусловлено бесконтрольным применением БАС. В совокупности они могут способствовать реализации широкого спектра противоправных актов – от криминальных эксцессов в сфере киберхулиганств и киберкраж, до опасных деяний террористической, шпионской и диверсионной направленности. Естественно, отмеченные особенности и проявления должны быть учтены при формировании комплексного подхода к управлению беспилотным транспортом, призванного обеспечить безопасность, надежность и эффективность транспортных операций.

Возникающие нарушения в процедурах функционирования систем управления (СУ) БАС требуют регулирующих влияний, ориентированных на все более развитые алгоритмические подходы и, в конечном итоге, возлагаемых на технологии ИИ.

Система угроз и уязвимостей безопасному управлению

Угрозы кибербезопасности – совокупность условий и факторов, создающих потенциальную опасность потери управления БАС, штатного функционирования или получения несанкционированного доступа к нему из-за целенаправленных вредоносных программно-аппаратных воздействий на СУ беспилотного транспорта.

Как отмечено, в современных условиях важную роль в СУ БАС играют технологии ИИ. Интеллектуальный ресурс используется для обработки информации, подготовки и принятия решений, непосредственного управления транспортным средством. Кроме того, ИИ может использоваться для обучения моделей и алгоритмов, участвующих в СУ БАС.

Вместе с тем реалии привели к необходимости учитывать уязвимости и формирующиеся на этой основе киберугрозы инфраструктуре, необходимой для СУ. В самом общем виде СУ интегрирует в себе подсистемы связи, хранения и обработки данных, организации и управления движением. В совокупности они обеспечивают ориентирование БАС в пространстве и корректное движение по маршруту.

В качестве подхода для формирования первичного перечня актуальных угроз кибербезопасности в рассматриваемой предметной сфере предлагается ориентироваться на Банк данных угроз (БдУ) ФСТЭК России (ubi.fstec.ru). Включение в указанный перечень типовых угроз для СУ БАС и определение их для каждого этапа ее жизненного цикла создает основу для создания и описания *базовой модели угроз* (БМУ). Исходя из обозначенного подхода, формируется перечень угроз, которые имеют наибольший уровень влияния в рамках анализируемых процессов.

Примерами таких угроз являются:

– УБИ.006: Угроза внедрения кода или данных;

– УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации;

– УБИ.011: Угроза деавторизации санкционированного клиента беспроводной сети;

– УБИ.023: Угроза изменения компонентов информационной системы;

– УБИ.030: Угроза использования информации об идентификации/аутентификации, заданной по умолчанию;

– УБИ.031: Угроза использования механизмов авторизации для повышения привилегий;

– УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными;

– УБИ.036: Угроза исследования механизмов работы программы;

– УБИ.047: Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке;

– УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

– УБИ.069: Угроза неправомерных действий в каналах связи;

– УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

– УБИ.074: Угроза несанкционированного доступа к аутентификационной информации;

– УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи.

Полный перечень угроз формируется путем добавления киберугроз, специфичных для СУ конкретных типов БАС.

Общий алгоритм формирования множества угроз кибербезопасности СУ БАС включает:

1) начальное формирование перечня киберугроз безопасности информации, циркулирующей в СУ БАС;

2) структурно-логический анализ множества угроз, систематизация и конкретизация;

3) верификация множества угроз, опираясь на опыт создания и эксплуатации СУ БАС;

4) дополнение множества угроз, применяя методы экспертных оценок полноты множества угроз и причинно-следственных связей;

5) верификация угроз и дополнение их множества методами имитационного моделирования;

6) дополнение множества угроз путем применения методов экспертных оценок;

7) верификация угроз и дополнение множества с применением натурных экспериментов;

8) формирование системы киберугроз безопасности защищаемой информации.

Основа построения подобного алгоритма приведена в виде последовательного перехода. Однако в процессе его работы возможны циклические повторы с организацией определенного количества итерационных действий.

Выполнение процедур анализа и обобщения приводит к выделению следующих условных групп угроз кибербезопасности БАС.

1. *Безопасность данных*:

– несанкционированный доступ к данным СУ БАС;

– фальсификация или подмена данных, связанных с принятием решений по управлению движением БАС (например, о маршрутном задании или данных об окружающей среде);

– внедрение вредоносных программ, которые могут влиять на СУ и приводить к сбоям или утечке информации.

2. *Безопасность связи*:

– подделка сигналов связи между БАС и СУ;

– внедрение вредоносных программ, нарушающих работу систем связи с целью перехвата управления БАС.

3. *Безопасность СУ*:

– ошибки в ПО, которые могут привести к сбоям или уязвимостям в СУ;

– ошибки идентификации БАС и элементов, взаимодействующих с СУ;

– уязвимости в аппаратном обеспечении, потенциально допускающие получение несанкционированного доступа к СУ БАС.

4. *Инфраструктурные угрозы безопасности*, которые могут отражать недостатки в системах:

– организации и управления движением, которые способны создавать сбои или уязвимости в СУ флотом БАС;

– связи, реализующиеся в их потере между БАС и внешней СУ.

5. *Безопасность систем ИИ*:

– внесение некорректных данных в целях манипуляции системой ИИ, преднамеренного искажения результатов работы и нарушения функционирования СУ БАС;

– ошибки различной природы в моделях обработки данных;

– получение конфиденциальной информации путем обмана ИИ;

– закладки в моделях в целях получения несанкционированного доступа к конфиденциальной информации, воздействия на результаты работы системы ИИ.

Конечно, приведенные обобщающие сведения не исчерпывают всего многообразия возможных типов и видов угроз. Поэтому могут быть иные частные проявления реальных и потенциальных угроз кибербезопасности.

Так, незаконная санкционная политика Запада осложняет доступ к международным базам уязвимостей и индикаторам компрометации, источникам данных об угрозах. Это приводит к «ослеплению» средств киберзащиты, не позволяя организовать их оптимальную систему.

К этому добавляются факторы эксплуатации зарубежного ПО и ресурсов Интернет, а также отказов в технической поддержке *IT*-оборудования и обновления ПО. Очевидно, в этих условиях возрастает вероятность реализации кибератак на СУ, а ее защита становится непростой задачей.

Поскольку уязвимости в СУ БАС могут быть внесены до начала эксплуатации, ее защиту необходимо обеспечить на всех этапах жизненного цикла:

– формирование требований;

– проектирование;

– разработка;

– ввод в действие;

– эксплуатация;

– вывод из эксплуатации.

В целях учета и систематизации всех факторов угроз безопасности СУ БАС и сфер проявления угроз необходимо разрабатывать модели угроз для каждого конкретного вида и класса БАС. С переходом на новые уровни автономности (УА) транспортных средств появляются новые уязвимости и новые угрозы в СУ. Их обобщенная характеристика объединена в таблице.

Таблица

Угрозы кибербезопасности интеллектуальной системе управления в зависимости от уровня автономности БАС

УА БАС	Характеристика уровня автономности	Угрозы СУ
УА-5	Полная автономность БАС. Пилот не требуется	Уровень 4 Угрозы, связанные с потерей контроля над системами ИИ
УА-4	Полные возможности самостоятельного вождения. Пилот контролирует и управляет удаленно по радиоканалам	Уровень 3 Угрозы, связанные с перехватом управления. Угрозы искажения данных, от ошибок в данных, закладки в моделях ИИ
УА-3	Ограниченные возможности самостоятельного вождения, БАС контролируется и при необходимости управляется пилотом	Уровень 2 Угрозы, связанные с возможным влиянием на корректность работы бортовых систем по каналам связи
УА-2	Частичная автоматизация и помощь водителю. Транспортным средством управляет компьютер	Уровень 1 Угрозы, связанные с работой бортового компьютера, ошибками ПО, уязвимостями аппаратных средств
УА-1	Ассистенты пилота помогают в сложных условиях движения, при этом пилот контролирует все (не предусмотрено автоматизированных систем вождения)	Уровень 0 Угрозы, связанные с некорректной работой ассистентов пилота
УА-0	Функций автоматизации и помощников нет. Транспортное средство полностью контролируется и управляется пилотом	Угрозы, связанные с работой внешних систем организации и управления движением: светофоры, информационные табло

Для учета всех возможных факторов и проявлений угроз безопасности СУ БТС необходимо разработать и поддерживать в актуальном состоянии модели угроз кибербезопасности для каждого вида и класса БТС, с учетом УА БТС. В целях обеспечения системности и единства подходов к решению вопросов кибербезопасности беспилотного транспортных средств (БТС), если говорить обобщенно, необходимо следовать системе моделей угроз (МУ) информационной безопасности, адаптированных к конкретным видам, типам и уровням автономности БТС.

Система МУ безопасности включает в себя три вида моделей:

– базовую МУ безопасности информации беспилотного транспорта, основанную на иерархии УА БТС;

– типовые МУ безопасности составных частей СУ БТС;

– частные (по видам БТС) модели угроз (ЧМУ).

Приведенные типы и классы применительно только к БАС обозначены следующим образом.

Типы БАС:

– С – самолетный;

– В – вертолетный;

– М – мультироторный;

– К – конвертоплан;

– Г – гибридный.

Классы БАС:

– СЛ – сверхлегкий (до 4 кг);

– Л – легкий (4–30 кг);

– С – средний (30–500 кг);

– Т – тяжелый (свыше 500 кг).

В организационном смысле БМУ является методической основой для:

– разработчиков БТС и разработчиков средств защиты информации БТС;

– организаций, выполняющих работы по проектированию систем контроля и управления беспилотным транспортом;

– организаций, осуществляющих оценку соответствия беспилотного транспорта требованиям защиты информации и его сертификации по требованиям регуляторов.

БМУ должна содержать описание объекта защиты в части структуры и функциональных характеристик СУ БТС, соответствующих им угроз безопасности информации и модели нарушителя, а также методические рекомендации по разработке типовых и частных МУ. Модель охватывает все стадии жизненного цикла БТС, в том числе – порядок разработки (проектирование, изготовление опытного образца и испытания), производства, эксплуатации и утилизации. Кроме того, она определяет порядок и условия разработки:

– типовых моделей угроз безопасности центров контроля и управления движением для типовых элементов в СУ БТС;

– частных (по видам БТС) моделей угроз объектов (элементов) СУ БТС.

Для поддержания моделей угроз всех видов в актуальном состоянии необходимо проводить их регулярное уточнение при:

– выявлении новых угроз, появлении новых способов и средств их реализации;

– при модернизации системы контроля и управления беспилотным транспортом, изменении структуры и (или) конфигурации ее инфокоммуникаций.

Если говорить кратко, основные результаты исследований авторов, полученные в последние два-три года, более глубоко и широко, по сравнению

с настоящей статьей, представлены в монографиях «Искусственный интеллект: противодействие киберпреступности» под ред. В.А. Минаева, К.М. Бондаря (Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2025. 256 с.) и «Риски топливно-энергетического комплекса России: современные угрозы и управление», подготовленной В.А. Минаевым, А.В. Мокшанцевым, А.С. Толпыгиным, А.О. Фаддеевым (М.: Академия ГПС МЧС России, 2025. 248 с.). В них освещаются задачи организации безопасного управления беспилотным транспортом, находящим все большее применение в борьбе с киберпреступностью, но в то же время и активно становящегося предметом реализации киберугроз.

В указанных монографиях и статьях авторов[1] представлены основные сведения по таким приложениям, как кибербезопасность БАС дистанционного мониторинга территорий; новые подходы к экспертно-криминалистической деятельности, в том числе обеспечения доказательственной базы киберпреступлений; интеграция с геоинформационными системами для совершенствования информационно-аналитического обеспечения раскрытия, расследования, профилактики киберпреступлений; автоматическое распознавание объектов и маршрутизация БАС, принятие решений по обеспечению их безопасности.

Показано, что перспективными направлениями исследований в области беспилотного транспорта являются:

– обоснование и выбор интеграционной шины отечественной разработки;

– разработка на базе технологий ИИ алгоритмов, программ, структур данных и протоколов взаимодействия, а также выбор технических решений по получению данных о состоянии БТС в центры контроля и управления их движением;

– опережающее развитие модели угроз и нарушителей, требований по обеспечению кибербезопасности применения беспилотников.

[1] Минаев В.А., Толпыгин А. С. Кибербезопасность и киберустойчивость беспилотных транспортных систем // Информация и безопасность. 2024. Т. 27. № 2. С. 177-184; 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; Минаев В.А., Толпыгин А.С., Бондарь К.М. Кибербезопасность беспилотных авиационных систем мониторинга лесных территорий // Информация и безопасность. 2024. Т. 27. № 4. С. 553-568; Толпыгин А.С., Минаев В.А., Куликов Л.С., Пахомов А.К. Искусственный интеллект – помощник цифровой полиции: возможности и перспективы // ЦИФРОПОЛ 2025. М., 2025. С. 98-105.