Инженерный вестник Дона, №10 (2025)
ivdon.ru/ru/magazine/archive/n10y2025/10471

Платформа анализа безопасности беспилотных автоматизированных систем

В.Д. Михайлова, М.А. Балеев

Южный федеральный университет, Таганрог

Аннотация: Цель исследования заключается в разработке платформы, которая позволяет проводить различные типы проверок для выявления слабых мест в подсистемах беспилотных автоматизированных систем. Методы исследования: при разработке платформы использовалась методика, основанная на построении онтологических моделей, которая позволила связать структурно-функциональные характеристики беспилотных автоматизированных систем с угрозами и уязвимостями, а также с атаками таких систем. Для сканирования радиочастотных диапазонов использовался метод распараллеливания процессов. Система принятия решений основана на методах оценки рисков. Результаты исследования: платформа позволяет оптимизировать процесс тестирования безопасности беспилотных автоматизированных систем. Для автоматизированной проверки используется база данных, включающая в себя каталог структурно-функциональных характеристик, угроз, уязвимостей, атак. Платформа может определить, каким типам структурно-функциональных характеристик соответствуют уязвимости беспилотных автоматизированных систем. Система, состоящая из отдельных компонентов (сенсор для сканирования беспилотных автоматизированных систем, интеллектуальная система активного анализа беспилотных автоматизированных систем). Сенсор для сканирования беспилотных автоматизированных систем реализован в виде малогабаритного устройства. Система интеллектуального активного анализа беспилотных автоматизированных систем реализована в виде программного обеспечения. Научная новизна заключается в разработке концепции системы анализа безопасности беспилотных автоматизированных систем на основе онтологических моделей и анализа радиочастотного диапазона для выявления уязвимых мест системы при проведении предэксплуатационных проверок.
Ключевые слова: анализ данных, статистика, атаки, риски, беспилотные автоматизированные системы.

Введение

Сегодня вопросы, связанные с безопасностью беспилотных автоматизированных систем (БАС), становятся актуальными. БАС используют в различных сферах жизни человека, в обеспечении охраны объектов и ведения разведывательных операций [1].

Авторы статьи [2] говорят о росте популярности беспилотных автоматизированных систем. Они применяются в критически важных миссиях (например, мониторинг инфраструктур), поэтому должны быть устойчивы к киберугрозам. Авторы описывают уязвимости в системе безопасности, выполняют атаку «Человек посередине» и вводят управляющие команды в скомпрометированный БАС.

Для противодействия угрозам в данной работе предложена модель для одноранговой сети с несколькими БАС. Целью этой модели является изучение среды одноранговой сети с несколькими БАС для выявления различных угроз. Эти угрозы проходят через модуль анализа угроз, который вычисляет оценку серьезности и сложности атаки. После рассчитывается рейтинг атаки. Уровень риска классифицируется, как высокий, средний и низкий. Разработанная платформа автоматизируют процесс выявления актуальных угроз и выработки сценариев атак на БАС. Отличие от существующих систем и методик состоит в том, что предлагаемая онтологическая модель, связывает понятия атак, угроз, уязвимостей и структурно-функциональные характеристики (СФХ) БАС. В предыдущих работах авторов была представлена методика оценки угроз для БАС [3, 4], а в статьях [5] рассмотрены сценарии атак на БАС.

Разработка архитектуры программно-аппаратной платформы

На рис. 1 представлена архитектура платформы для анализа защищенности БАС. Архитектура включает три основных уровня, которые, в свою очередь, включают в себя различные компоненты в соответствии с их функциональностью.

1. Физический уровень управления - исполнительные механизмы, датчики и аппаратные модули для сбора данных о БАС. В данной реализации ключевой компонент — радиочастотный модуль HackRF One SDR (Software-defined radio), работающий в двух режимах. Первое направление – анализ радиочастотного спектра (РС). Задачи: 1) Анализ радиочастот. 2) Сканирование радиочастотных диапазонов методом распараллеливания процессов. 3) Формирование файлов для подачи на вход нейросети для обнаружения активности. Второе направление — реализация сценариев атак и проверок БАС. Задачи: 1) Генерация необходимого сигнала для анализа восприимчивости к атаке глушения. 2) Автоматизация процесса атаки на

глобальную навигационную систему для проверки восприимчивости к этой атаке со стороны БАС. 3) Автоматизация атак.

2. Интеллектуальный уровень управления - нейронная сеть для классификации данных.

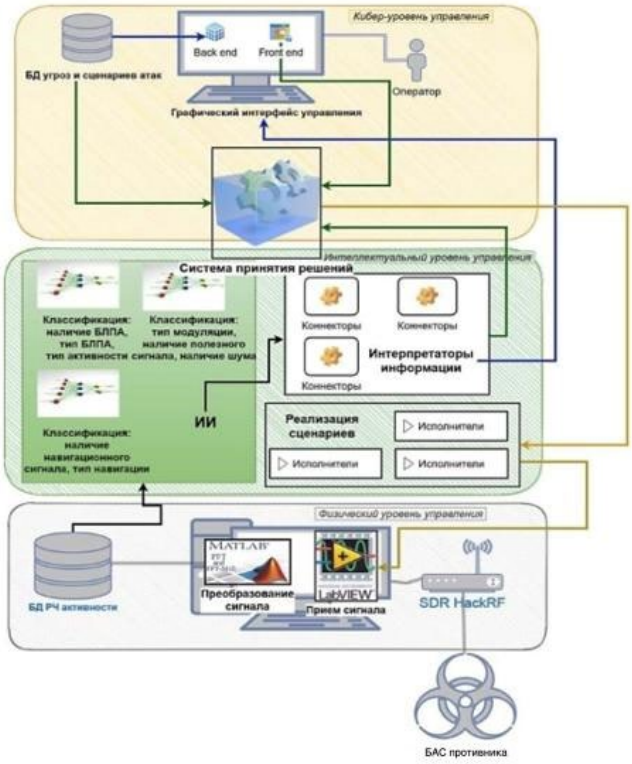

Рис. 1. – Архитектура платформы для автоматизированного анализа защищенности БАС

3. Киберуровень - система принятия решений, анализирующую сценарии атак; графический интерфейс для данных и взаимодействия с оператором [6]; база угроз, уязвимостей и атак с сопоставлением ключевых признаков (СФХ).

Разработка базы данных угроз, уязвимостей атак на основе онтологической модели

База данных (БД) использует связи между концептами для: интеллектуального поиска угроз по заданным СФХ БАС;

автоматического/ручного ввода данных о БАС; распознавания СФХ и сопоставления с потенциальными атаками. Согласованность каталогов (угроз, атак, уязвимостей, СФХ) ускоряет идентификацию релевантных атак. На рис. 2 показана структура разработанной системы.

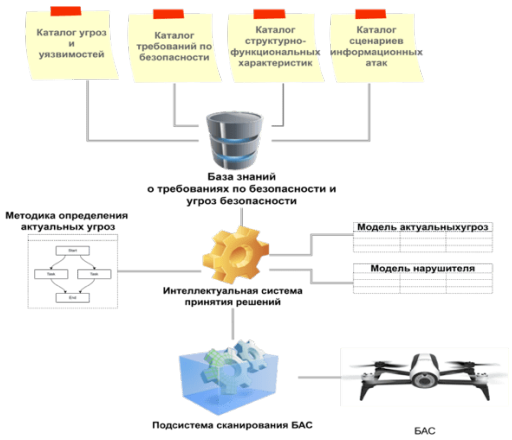

Рис. 2. – Схема интеллектуальной системы идентификации угроз

На рисунке 2 видно, что для принятия решений об угрозах для БАС необходимо обнаружить БАС и собрать информацию о нем. Необходимо определить наличие уязвимостей у БАС, и сценария атак, СФХ.

Разработка интеллектуальной системы управления безопасностью БАС

Пользовательский интерфейс осуществляет взаимодействие с оператором, генерацию команд и отображение результатов. Архитектура изображена на рис. 3.

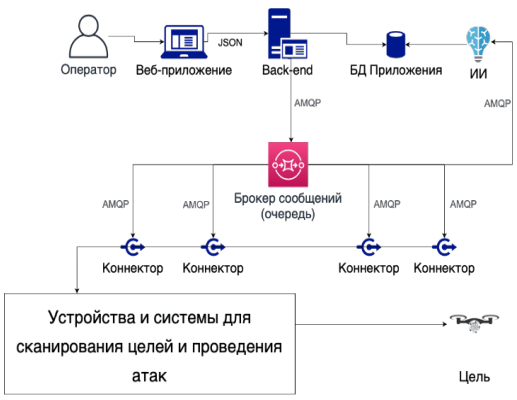

Рис. 3. – Схема ПО для тестирования защищённости БАС

Разработка сценариев исследования БАС

При тестировании атак на БАС были реализованы угрозы на канал управления БАС, на систему глобальной навигации. Первый сценарий атаки - отказ в обслуживании для канала управлении БАС.

1. При сканировании Wi-Fi диапазона определяется используется ли БАС в режиме точки доступа для управления с мобильного устройства. Если точка доступа обнаруживается, атака продолжается по шагу 3, если нет, то шаг 2.

2. Если точек доступа, создаваемых БАС, не обнаружено, то тогда может быть несколько вариантов действий.

2.1 БАС может подключаться к точке доступа и управляться дистанционно по каналу Wi-Fi [7]. Это можно обнаружить путем сканирования диапазона Wi-Fi и анализа MAC-адреса клиентов, подключенных к ней.

2.2 Для БАС, работающих на протоколах связи (2.4 ГГц, 915 МГц, 5 ГГц и др.) [8], их поиск каналов управления выполняется с помощью HackRF и Программное обеспечение (ПО) RF Analyzer [9]. Если сигналы обнаружены, процесс переходит к этапу атаки (шаг 3).

БАС коммерческого типа, передающие видеопоток, менее подвержены изменению ширины полосы пропускания. Это связано с тем, что для передачи постоянного видеопотока необходимо постоянно занимать каналы или частоты передачи данных и передавать данные с высокой интенсивностью [10, 11]. В исследовании также был задействован (First Person View) FPV БАС. Работа БАС на частоте, передающий видеопоток, 1150 МГц показана на радиочастотном спектре на рис. 4. Вывод: при измерении радиочастотного спектра указанной частоты при активном БАС:

1150 МГц – присутствовали отклонения сигнала, резкие колебания частоты, рядом с исследуемой частотой идет передача сигнала от FPV БАС [12-14].

(а)

(б)

Рис. 4. – Сканирование РС во время (а) работающего FPV (б) DJI Mavic Air на частоте 2467 МГц

3. Проведение атаки отказ в обслуживании.

3.1 При использовании БАС точки доступа Wi-Fi возможна атака деаутентификации, где клиенты отключаются от сети. В результате легитимный оператор теряет связь с БАС.

3.2 Если управление осуществляется по другому протоколу, применяется атака зашумления с помощью HackRF. Генерация мощного сигнала подавляет легитимный канал связи, приводя к потере управления.

4. Оценка результатов атаки. Легитимный оператор БАС должен потерять возможность управления БАС. При атаке уровень шума значительно повышается и достигает 200 дБ, а уровень сигнала составляет от 0–20% [15].

Данный сценарий атаки был реализован для трех типов коммерческих БАС: ARDrone 2.0 Parrot, DJI Mavic Air и БАС на базе полетного контроллера

(ПК) PixHawk 4. В результате атаки владелец теряет контроль над БАС. При реализации сценария на DJI Mavic Air наблюдалось два варианта событий. В первом - БАС начинал посадку даже после завершения атаки, оператор не мог подключиться к БАС. Второй - БАС пытался вернуться на точку, откуда он взлетал, это происходило в случае, если точка была изначально записана оператором или оператор мог перехватить управление БАС, но он не воспринимал команды, а стремился вернуться на точку взлета.

Второй сценарий – перехват управления БАС. Для осуществления перехвата управления БАС необходимо проделать первые три шага сценария атаки отказа в обслуживании.

1. Атака направлена на БАС, работающий на частоте 915 МГц и на протоколе MAVLink для связи с наземной станцией управления. Настройки мощности передачи, каналов и частот загружаются в радиомодем HM-TRP и отображаются в программе Mission Planner. Ключевым параметром является Net ID, позволяющий нескольким устройствам работать в одном радиоканале без помех [16]. Атака применима к БАС на ПК Pixhawk и на Arducopter.

2. Если обнаружено БАС под управлением ARDrone 2.0 Parrot, запускается скрипт, помогающий управлять автоматически утилитой aircrack-ng. Далее сетевая карта переводится в режим монитора и производится деаутентификация нужных MAC-адресов.

3. Атака на БАС DJI происходит схожим образом, за исключением того, что БАС не дает подключиться сразу двум пользователям одновременно к нему, а также не дает после сброса соединения подключиться к нему с помощью мобильного телефона и приложения, даже легитимному пользователю.

Третий сценарий – подмена навигационного сигнала на систему глобальной навигации GPS. В ходе эксперимента была смоделирована атака GPS-спуфинг с использованием радиочастотного модуля HackRF One, в рамках которой проведено 100 тестовых испытаний. В режиме стабилизации

аппарат, пытаясь компенсировать искусственно созданное смещение, входит в режим повышенной нагрузки на двигатели. При полете по маршруту БАС, получая некорректные навигационные данные, отклоняется от заданной траектории, при этом система автопилота пытается безуспешно вернуть аппарат на курс.

Разработка логических связей системы принятия решений для анализа безопасности БАС

Для построения логических связей для объединения модулей был построен граф связей. Данный граф включает в себя следующие сущности: метрики, правила обнаружения, правила реагирования, аномалии, сценарии реагирования [17]. На рис. 5 представлен граф связности для системы принятия решений с целью анализа безопасности БАС.

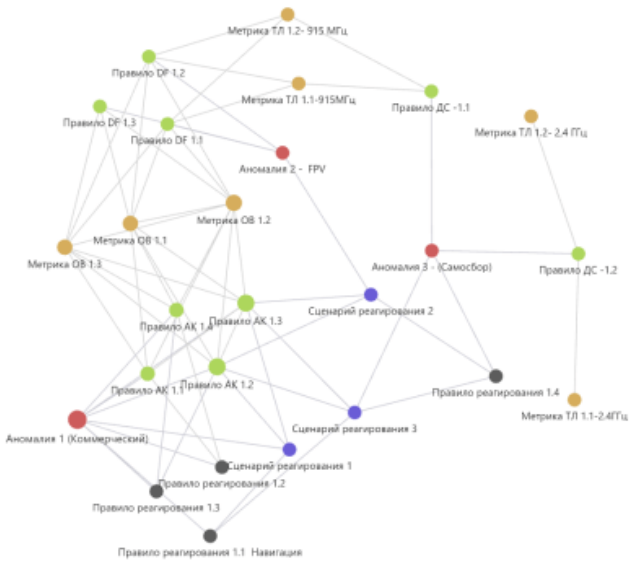

Рис. 5. – Граф связности системы принятия решений

Метрика – это правила анализа, получаемого от компонентов физического уровня. Сигналы приходят в виде столбчатой диаграммы значений. Получаемые значения соответствуют интенсивности передачи данных, или мощности приминаемого сигнала [18, 19].

Метрики позволяют оценить характеристики принимаемых сигналов, отличить тип сигнала. Правило обнаружения сочетает в себе комбинации метрик и порогов обнаружения для детектирования одного из типов аномалий.

Описание метрик для детектирования БАС.

Метрика ОВ 1.1 - применяется для обнаружения видеопотока. Оцениваем устойчивость всплеска радиочастотной активности.

После каждой итерации собирается массив пиков, далее определяются середины пиков: середина пика = (end - start) /2.

Затем проводится сравнительный анализ центров всплесков радиочастотной активности. Если один и тот же центр появляется на протяжении трех итераций, то делается вывод о стабильности всплеска радиочастотной активности.

Метрика ОВ 1.2 - позволяет выделять всплески на общей радиочастотной картине. После выделения всплеска, считается его ширина путем нахождения разницы между индексом конечной и начальной частот.

Hill = {start: int, end: int, length: end - start}

Далее выделяются основные булевы высказывания:

- A = Ширина всплеска радиочастотой активности попадает в диапазон [5, 12], - B = Ширина всплеска радиочастотной активности попадает в диапазон [25, 60], - C = всплесков радиочастотной активности нет, то есть ширина меньше 5.

В соответствии с высказываниями выделим основные гипотезы:

- A & (!B || B) & !C => обнаруженный БАС передаёт видеопоток. - !A & B & !C => необходим анализ пространства с учетом средней высоты пика, - !A & !B & C => БАС не обнаружено.

Метрика ОВ 1.3 - расчет метрики работает на основе алгоритма, представленного в [Метрика ОВ 1.2]. Оценка высоты пика. Оценивается

высота пика, или RSSI, то есть, насколько пик мощный или сигнал стабильный.

Метрика ТЛ 1.1–2.4 ГГц - включает в себя процентный подсчет числа ненулевых частот пространства. Измеряется число частот, на которых зафиксирована активность радиоканала.

Метрика ТЛ 1.1-915МГц - измеряется число частот, на которых зафиксирована активность радиоканала в определённом диапазоне частот.

Метрика ТЛ 1.2–2.4 ГГц - высота сигнала не превышает порог.

Метрика ТЛ 1.2–915 МГц - метрика учитывает выпадающие значения частот на диапазоне 915 МГц, если любая частота в диапазоне [901, 920] превышает порог, делается вывод о присутствии БАС самособранного типа.

Описание правил обнаружения для детектирования БАС (табл. 1).

Таблица 1

Описание правил

Правило	**Описание**	**Связанные метрики и правила**	**Выражение**
1	2	3	4
Правило АК 1.1	БАС считается, как Аномалия 1, если его можно обнаружить согласно правилу, которое подходит для обнаружения видеопотока на частоте 2,4 ГГц	[Метрика ОВ 1.1] - A [Метрика ОВ 1.2] - B [Метрика ОВ 1.3] - C	1. (A === true) and (5 <= B <= 13) => true 2. (C >= 30) and (B >= 20) => true
Правило АК 1.2	БАС считается, как Аномалия 1, если его можно обнаружить согласно правилу, которое подходит для обнаружения видеопотока на	[Метрика ОВ 1.1] [Метрика ОВ 1.2] [Метрика ОВ 1.3]	C > 20 => true

	частоте 5,8 ГГц		
Правило АК 1.3	БАС считается, как Аномалия 1, если его можно обнаружить согласно правилу, которое подходит для обнаружения видеопотока на частоте 2.4 ГГц и 5.8	[Метрика ОВ 1.1] - A [Метрика ОВ 1.2] - B [Метрика ОВ 1.3] - C [Правило АК 1.1] - D (x1, x2, x3) [Правило АК 1.2] - E (x1, x2, x3)	(D(A, B, C) === true) or (E(A, B, C)) => true

1	2	3	4
Правило АК 1.4	БАС считается Аномалия 1, если есть активность, которая считается телеметрией на частоте 2,4 ГГц и есть активность на частоте 5,8 ГГц, которая считается видеопотоком	[Метрика ОВ 1.1] [Метрика ОВ 1.2 [Метрика ОВ1.3]	-
Правило ДС -1.1	Правило 1 Обнаружена активность, соответствующая передаче телеметрии на частоте 433 МГц, 915 МГц	[Метрика ТЛ 1.2–915 МГц] - A [Метрика ТЛ 1.1-915МГц]-B	(A === true) and (B >= 15) => true
Правило ДС -1.2	Правило 1 Обнаружена активность, которая соответствует передаче телеметрии на частоте 2.4 ГГц	[Метрика ТЛ 1.2–2,4 ГГц] - A [Метрика ТЛ 1.1-2.4ГГц] – B	(A === true) and (B >= 15) => true

Правило DF 1.1	Обнаружена активность, соответствующая передаче телеметрии на частоте 915 МГц и передаче видео на частоте 2,4 ГГц	[Метрика ТЛ 1.1-915МГц] [Метрика ТЛ 1.2- 915 МГц] или [Метрика ОВ 1.1] [Метрика ОВ 1.3] [Метрика ОВ 1.2]	-
Правило DF 1.2	Обнаружена активность, соответствующая передаче телеметрии на частоте 915 МГц и передаче видео на частоте 5,8 ГГц	[Метрика ТЛ 1.1-915МГц] [Метрика ТЛ 1.2- 915 МГц] или [Метрика ОВ 1.1] [Метрика ОВ 1.3] [Метрика ОВ 1.2]	-
Правило DF 1.3	Обнаружена активность, соответствующая передаче видео на частоте 915 МГц	[Метрика ОВ 1.1] - [Метрика ОВ 1.3] [Метрика ОВ 1.2]	-

Описание аномалий БАС отражено в табл. 2.

Таблица 2

Описание аномалий

Аномалия	**Описание**	**Связанные правила и аномалия**	**Выражение**
Аномалия 1 (Коммерческий БАС по типу Mavic Air)	Коммерческий БАС работает на двух частотах 2,4 и 5,8. При этом БАС передает видео.	[Правило АК 1.4] [Правило АК 1.2] [Правило АК 1.3] [[Правило АК 1.1]	На рис. 6 (а) представлен локальный граф, который связывает Аномалию 1 с другими сущностями графа
Аномалия 2 – FPV	FPV БАС работает на частотах 915 или 433 для передачи телеметрии, видео	[Правило DF 1.1] [Правило DF 1.3]	Локальный граф связности для Аномалии 2 представлен на

	может передаваться на 915 МГц, 2,4 ГГц , 5,8 ГГц	[Правило DF 1.2]	рис. 6 (б)
Аномалия 3 - (Самосборный)	БАС собственной сборки с функцией автономного полета не использует передачу видео, использует телеметрию для связи с оператором	[Правило ДС - 1.1] [Правило ДС - 1.2]	Локальный граф связности для аномалии 3 представлен на рис. 6 (в).

(а)

(б)

(в)

Рис. 6. – Локальный граф для Аномалии 1 (а). Аномалии 2 (б). Аномалии 3 (в)

Заключение

Разработана и реализована архитектура и концепция системы. Разработанная архитектура имеет следующие преимущества: позволяет увеличить количество модулей и коннекторов, является кроссплатформенной, масштабируемой и при необходимости может быть переконфигурирована. В результате данная система позволяет автоматизировать различные процессы. Создан интерфейс для автоматизации атак. Разработанный для оператора интерфейс может использоваться с целью тестирования процесса проведения атак и разработки сценариев атак на БАС. Реализованы возможность обнаружения БАС в радиодиапазоне, возможность сканирования радиочастотного диапазона и обнаружения активности БАС, а также возможность сбора данных о БАС и составления БД для обучения нейросети. Сценарии атак были протестированы на экспериментальном стенде и проанализирована эффективность реализованных атак. В результате был получен набор угроз и атак для экспериментальных стендов.

Результаты испытаний в лабораторных условиях в табл. 3, 4, 5 и 6.

Таблица 3

Результаты, полученные в лабораторных условиях, в присутствии БАС

	Всего ситуаций	**Срабатываний**	**% корректности**	**% ошибок**
Передача данных на 2,4 ГГц	362	321	88,91	11,8
Передача данных на 5,8 ГГц	399	399	100	0
Передача данных на 915 МГц	88	88	100	0

Коммерческий	172	158	91,6	8,4
FPV	130	128	98,46	1,57
Самособранный	125	118	94,4	5,6
Среднее			95,1	4,4

Таблица 4

Результаты, полученные в лабораторных условиях, в отсутствие БАС

	Всего ситуаций	**Срабатываний**	**% корректности**	**% ошибок**
БАС отсутствует	902	74	91,79600887	8,203991131

Таблица 5

Результаты испытаний в полевых условиях в присутствии БАС

	Всего ситуаций	**Срабатываний**	**% корректности**	**% ошибок**
Передача данных на 2,4 ГГц	150	147	98	2
Передача данных на 5,8 ГГц	150	141	94	6
Передача данных на 915 МГц	150	149	99	1
Коммерческий БАС	150	148	98	8,4
FPV БАС	150	146	97	1,57
Самособранный	150	143	95,3	5,6
Среднее			97	3

Таблица 6

Результаты испытаний в полевых условиях в отсутствие БАС

	Всего ситуаций	**Срабатываний**	**% корректности**	**% ошибок**

БАС отсутствует	150	0	100	0

Таким образом, платформа позволяет определять тип БАС, частоту на которой передаются данные и тип передаваемых данных. На основе собранной информации формируется сценарий противодействия, затем он тестируется и появляется возможность оценить уровень защищенности БАС, а также модифицировать БАС таким образом, чтобы снизить существующие риски. Автоматизация упрощается процессом ввода в эксплуатацию БАС.

Работа выполнена в рамках научно-исследовательского проекта № ВнГр/24-01-КТ «Разработка демонстрационной модели БПЛА с повышенной отказоустойчивостью».

Литература

1. Best K. L., Schmid J., Tierney S., Awan J., Beyene N. M., et al. How to Analyze the Cyber Threat from Drones Background, Analysis Frameworks, and Analysis Tools. Published by the RAND Corporation. Santa Monica. Calif. 2020. URL: academia.edu/70058179/How_to_Analyze_the_Cyber_Threat_from_Drones_Background_Analysis_Frameworks_and_Analysis_Tools
2. Basan E., Basan A., Nekrasov A., Fidge C., Sushkin N., Peskova O. GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence. Drones. 2022. P. 8.
3. Basan A., Basan E. The Methodology for assessing information security risks for robotic systems. CEUR Workshop Proceedings. 2020. Pp. 30–35.
4. Basan E., Basan A., Nekrasov A., Fidge C., Ishchukova E., Basyuk A., Lesnikov A. Trusted operation of cyber-physical processes based on assessment of the system's state and operating mode. Sensors. 2023. Vol. 23. P. 4.

5. Basan, E.S., Sushkin, N.A., Babenko, L.K. Methodology for Detecting Attacks in the Context of Destructive Influences. In Proceedings of the 2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE). Novosibirsk. 2023. Pp. 1120–1124.
6. Basan, E., Basan, A., Nekrasov, A., Gamec, J., Gamcová, M. A self-diagnosis method for detecting UAV cyber-attacks based on analysis of parameter changes. Sensors. Switzerland. 2021. Pp. 1–17.
7. Griffiths H., Baker C., An Introduction to passive radar. Publisher: IEEE. 2022. URL: books.google.ru/books?id=DJmuDgAAQBAJ&redir_esc=y
8. Mattei F. Enhanced radar detection of small remotely piloted aircraft in U-space scenario. Materials Research Proceedings. 2023. Pp 15–20.
9. Martelli T., Filippini F., Colone F. Tackling the different target dynamics issues in counter drone operations using passive radar. IEEE International Radar Conference. 2020. Pp 512–517.
10. Souli, N., Theodorou, I., Kolios, P. Ellinas, G. Detection and tracking of rogue UAS using a novel real-time passive radar system. Conference on Unmanned Aircraft Systems. 2022. Pp 576–582.
11. Larrat M, Sales C. Classification of Flying Drones Using Millimeter-Wave Radar: Comparative Analysis of Algorithms Under Noisy Conditions. Sensors. 2025. URL: doi.org/10.3390/s25030721.
12. Mohammed, A.B., Fourati, L.C., Fakhrudeen, A.M. Comprehensive systematic review of intelligent approaches in UAV-based intrusion detection, blockchain, and network security. Comput. Netw. 2023. 239.
13. Seidaliyeva U, Ilipbayeva L, Taissariyeva K, Smailov N, Matson ET. Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review. Sensors. 2024. URL: doi.org/10.3390/s24010125.

14. Solaiman S, Alsuwat E, Alharthi R. Simultaneous Tracking and Recognizing Drone Targets with Millimeter-Wave Radar and Convolutional Neural Network. Applied System Innovation. 2023. URL: doi.org/10.3390/asi6040068.
15. Dumitrescu C, Minea M, Costea IM, Cosmin Chiva I, Semenescu A. Development of an Acoustic System for UAV Detection. Sensors. 2020. URL: doi.org/10.3390/s20174870.
16. Song C, Li H. An Acoustic Array Sensor Signal Recognition Algorithm for Low-Altitude Targets Using Multiple Five-Element Acoustic Positioning Systems with VMD. Applied Sciences. 2024. URL: doi.org/10.3390/app14031075
17. Chen T, Yu J, Yang Z. Research on a Sound Source Localization Method for UAV Detection Based on Improved Empirical Mode Decomposition. Sensors. 2024. URL: doi.org/10.3390/s24092701.
18. Tejera-Berengue, D., Zhu-Zhou, F., Utrilla-Manso, M., Gil-Pita, R., Rosa-Zurera, M. Acoustic-Based Detection of UAVs Using Machine Learning: Analysis of Distance and Environmental Effects. In Proceedings of the 2023 IEEE Sensors Applications Symposium (SAS). Ottawa. 2023. Pp. 1–6.
19. Тихонов А.М. Платформа для обмана злоумышленника - критерии её функциональности, сильные и слабые стороны, тренды // Инженерный вестник Дона, 2025, №7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10229.

References

1. Best K. L., Schmid J., Tierney S., Awan J., Beyene N. M., et al. How to Analyze the Cyber Threat from Drones Background, Analysis Frameworks, and Analysis Tools. Published by the RAND Corporation. Santa Monica. Calif. 2020. URL:

academia.edu/70058179/How_to_Analyze_the_Cyber_Threat_from_Drones_Background_Analysis_Frameworks_and_Analysis_Tools

2. Basan E., Basan A., Nekrasov A., Fidge C., Sushkin N., Peskova O. GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence. Drones. 2022. P. 8.
3. Basan A., Basan E. The Methodology for assessing information security risks for robotic systems. CEUR Workshop Proceedings. 2020. Pp. 30–35.
4. Basan E., Basan A., Nekrasov A., Fidge C., Ishchukova E., Basyuk A., Lesnikov A. Trusted operation of cyber-physical processes based on assessment of the system's state and operating mode. Sensors. 2023. Vol. 23. P. 4.
5. Basan, E.S., Sushkin, N.A., Babenko, L.K. Methodology for Detecting Attacks in the Context of Destructive Influences. In Proceedings of the 2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE). Novosibirsk. 2023. Pp. 1120–1124.
6. Basan, E., Basan, A., Nekrasov, A., Gamec, J., Gamcová, M. A self-diagnosis method for detecting UAV cyber-attacks based on analysis of parameter changes. Sensors. Switzerland. 2021. Pp. 1–17.
7. Griffiths H., Baker C., An Introduction to passive radar. Publisher: IEEE. 2022. URL: books.google.ru/books?id=DJmuDgAAQBAJ&redir_esc=y
8. Mattei F. Enhanced radar detection of small remotely piloted aircraft in U-space scenario. Materials Research Proceedings. 2023. Pp 15–20.
9. Martelli T., Filippini F., Colone F. Tackling the different target dynamics issues in counter drone operations using passive radar. IEEE International Radar Conference. 2020. Pp 512–517.

10. Souli, N., Theodorou, I., Kolios, P. Ellinas, G. Detection and tracking of rogue UAS using a novel real-time passive radar system. Conference on Unmanned Aircraft Systems. 2022. Pp 576–582.
11. Larrat M, Sales C. Classification of Flying Drones Using Millimeter-Wave Radar: Comparative Analysis of Algorithms Under Noisy Conditions. Sensors. 2025. URL: doi.org/10.3390/s25030721.
12. Mohammed, A.B., Fourati, L.C., Fakhrudeen, A.M. Comprehensive systematic review of intelligent approaches in UAV-based intrusion detection, blockchain, and network security. Comput. Netw. 2023. p. 239.
13. Seidaliyeva U, Ilipbayeva L, Taissariyeva K, Smailov N, Matson ET. Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review. Sensors. 2024. URL: doi.org/10.3390/s24010125.
14. Solaiman S, Alsuwat E, Alharthi R. Simultaneous Tracking and Recognizing Drone Targets with Millimeter-Wave Radar and Convolutional Neural Network. Applied System Innovation. 2023. URL: doi.org/10.3390/asi6040068.
15. Dumitrescu C, Minea M, Costea IM, Cosmin Chiva I, Semenescu A. Development of an Acoustic System for UAV Detection. Sensors. 2020. URL: doi.org/10.3390/s20174870.
16. Song C, Li H. An Acoustic Array Sensor Signal Recognition Algorithm for Low-Altitude Targets Using Multiple Five-Element Acoustic Positioning Systems with VMD. Applied Sciences. 2024. URL: doi.org/10.3390/app14031075.
17. Chen T, Yu J, Yang Z. Research on a Sound Source Localization Method for UAV Detection Based on Improved Empirical Mode Decomposition. Sensors. 2024. URL: doi.org/10.3390/s24092701.

18. Tejera-Berengue, D., Zhu-Zhou, F., Utrilla-Manso, M., Gil-Pita, R., Rosa-Zurera, M. Acoustic-Based Detection of UAVs Using Machine Learning: Analysis of Distance and Environmental Effects. In Proceedings of the 2023 IEEE Sensors Applications Symposium (SAS). Ottawa. 2023. Pp. 1–6.
19. Tihonov A.M. Inzhenernyj vestnik Dona, 2025, №7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10229.

Дата поступления: 23.07.2025

Дата публикации: 26.09.2025