Инженерный вестник Дона, №12 (2025)
ivdon.ru/ru/magazine/archive/n12y2025/10619

Исследование защиты канала передачи команд управления от перехвата в беспилотных воздушных судах

А.В. Смахталин[1], А.М. Ахметвалеев[1,2]

[1]Московский ордена Почета университет МВД России имени В.Я. Кикотя, Москва
[2]Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань

Аннотация: В статье приведены результаты исследования защищенности канала передачи команд управления беспилотных воздушных судов (БВС) на примере дрона с видом от первого лица. Исследования проводились в безэховой экранированной камере специализированного полигона сертифицированным измерительным оборудованием. Представлены результаты измерений спектральной панорамы и возможность пассивного перехвата сигналов в радиоэфире. Показана актуальность обеспечения безопасной эксплуатации БВС, а также уязвимость открытого протокола быстрой беспроводной связи дальнего действия к перехвату управления. Приведены рекомендации по использованию криптографических алгоритмов для нейтрализации угрозы безопасности.
Ключевые слова: беспилотное воздушное судно, протокол быстрой беспроводной связи дальнего действия, псевдослучайная перестройка рабочей частоты, программно определяемый радиоприёмник, безопасная эксплуатация, защита информации, уязвимости, несанкционированный доступ, перехват управления, идентификационная фраза.

Введение

Беспилотные воздушные суда стремительно вошли в различные сферы деятельности человека: от любительской фотосъемки до зондирования участков местности [1,2]. Использование беспилотных воздушных судов (БВС) в деятельности органах внутренних дел Российской Федерации является важной составляющей [3-5], направленной на расширение функциональных возможностей правоохранительной деятельности по предотвращению правонарушений, покушений на государственное и частное имущество, а также на поддержание общественной безопасности.

Вместе с тем, БВС, являясь специальными средствами, накладывают требования по обеспечению безопасной эксплуатации [5], в том числе с учётом требований информационной безопасности [3,6]. Для современных БВС характерны угрозы информационной безопасности, присущие компьютерным технологиям: перехват управления, искажение передаваемых данных, отказ в доступе из-за физических вмешательств и т.д. Уязвимости в

первую очередь связаны с недостатками в реализации протоколов связи БВС. Использование незащищенных протоколов в управлении БВС создает значимый риск безопасности [7], что и обуславливает необходимость проведения исследований и разработки систем защиты информации от несанкционированного доступа и другого вмешательства [3,8,9].

В данной статье приводятся результаты исследования канала передачи команд управления от перехвата, проведенные на базе специализированного полигона технической защиты информации Московского ордена Почета Университета МВД России имени В.Я. Кикотя.

Методология

Для проведения исследования использован БВС типа дрон с видом от первого лица (англ. First Person View), весом 600 гр, функционирующий на базе контроллера производства компании Diatone, программная часть которого основана на специализированном протоколе быстрой беспроводной связи дальнего действия (англ. Express Long Range System – ELRS) – проект с открытым исходным кодом для управления большинства популярных БВС. В качестве станции управления БВС использовался пульт марки RADIOMASTER, рабочая частота которого лежит в диапазоне 2,4–2,48 ГГц. Устройством воспроизведения видеосигнала выступил видеошлем марки 9IMOD с 5-дюймовым жидкокристаллическим дисплеем с разрешением 800 на 480, работающий на частотах 5,8 ГГц.

Диапазон рабочих частот контроллера: 2,4 ГГц и 5,8 ГГц для связи «аппарат управления – дрон» и передачи видеоданных, соответственно. ELRS характеризуется, прежде всего, частотным расширением спектра с прыжками по частотам (англ. Frequency-Hopping Spread Spectrum – FHSS). Это обеспечивает постоянную синхронизацию БВС с пультом оператора и псевдослучайную смену частоты, в пределах выделенной полосы, для затруднения несанкционированного доступа. Псевдослучайный выбор

частоты обусловлен сопряжением устройств, зависящим от «пароля» – идентификационной фразы, запрограммированной в прошивке БВС и настройках пульта управления.

Исследование проводилось в безэховой экранированной камере III-класса (БЭК), обеспечивающей изоляцию от внешних радиопомех и отражений, в соответствии с ГОСТ 30373-95/ГОСТ Р 50414-92. Для измерений параметров электромагнитных излучений применялась сертифицированная ФСТЭК РФ автоматизированная система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок «Сигурд-А10» ГК «Маском», в составе анализатора спектра R&S FSH13 (рабочий диапазон частот от 9 кГц до 13,6 ГГц), измерительной рупорной широкополосной антенны П6-223 (диапазон частот измерения от 0,8 до 18 ГГц) и специального программного обеспечения Сигурд-Лайт.

Комплект оборудования дрона размещался в объеме дистанционно управляемого поворотного стола, расположенного в центре БЭК. Схема размещения и подключения оборудования представлена ниже.

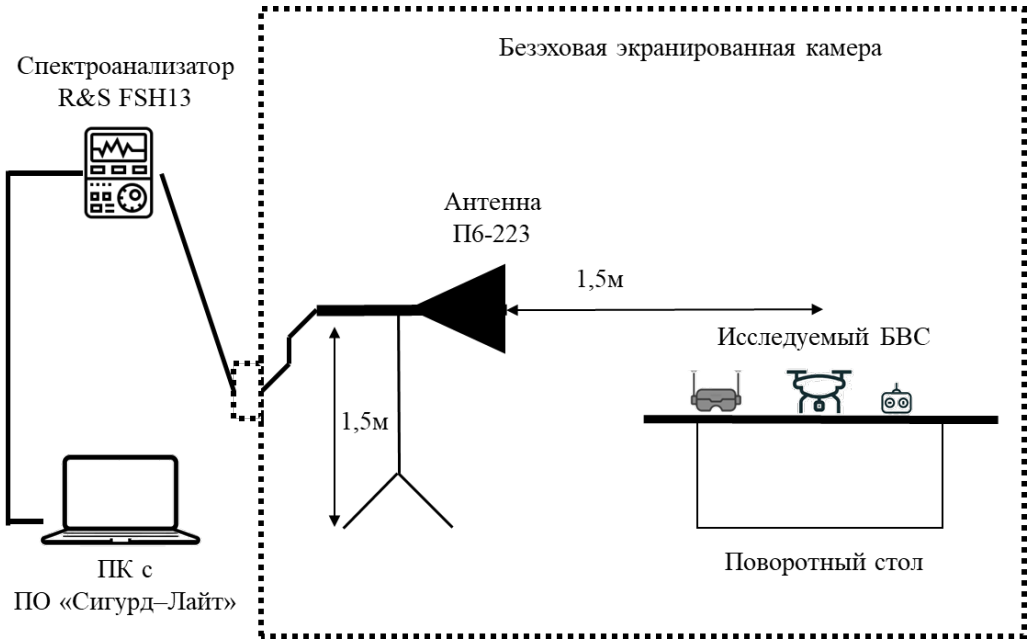


Рис. 1. – Схема размещения и подключения оборудования

Антенна П6-223 устанавливалась на дистанции 1,5 м от центра поворотного стола и на такой же высоте от уровня пола до ее геометрического центра. Комплектом проводов выход антенны подключался ко входу спектроанализатора, который, в свою очередь, по локальной вычислительной сети управлялся с персонального компьютера.

Фото размещения исследуемого и измерительного оборудования приведены на рисунке 2.

Рис. 2. – Фото размещения оборудования в БЭК

Измерения осуществлялись в круговой пространственной ориентации поворотного стола в 360° с интервалом шага в 30° для каждого вида поляризации антенны (вертикальная, горизонтальная, наклонная), что соответствует 36 точкам проведения измерений. В качестве результата фиксировался максимально измеренное значение принятого сигнала.

Перед началом измерения в БЭК осуществлен замер радиообстановки, в последующем принятый за уровень естественных шумов с усреднением 5 последовательных измерений.

В момент измерения дрон и комплект оборудования к нему находились во включенном состоянии в режиме ожидания и передачей видеоинформации на видеошлем.

Диапазон частот для поиска и анализа сигналов – от 2 до 6 ГГц. Поиск сигнала осуществлялся пиковым детектором с накоплением в 20 измерений. Фильтры полос разрешения и видеосигнала составили 100 и 300 кГц, соответственно, а полоса обзора частот – 44 МГц. Порог обнаружения сигнала составил 5 дБ относительно уровня радиообстановки.

После автоматического этапа оператором проведено ручное обследование наиболее сильных выявленных спектральных компонентов, чтобы привязать их к известным источникам (управление, видео и пр.).

С целью тестирования БВС путем моделирования реализации актуальных угроз оценки возможностей несанкционированного доступа к нему использовался программно-определяемый радиоприёмник марки HackRF One, предназначенный для приёма и передачи радиосигналов в диапазоне частот от 1 МГц до 6 ГГц. Задача моделирования заключалась в записи «сырых» данных сигнала управления ELRS и дальнейшего их воспроизведения в радиоэфире для имитации сигналов пульта.

Результаты

В результате проведенных измерений и анализа спектра сигнала получена следующая спектральная панорама.

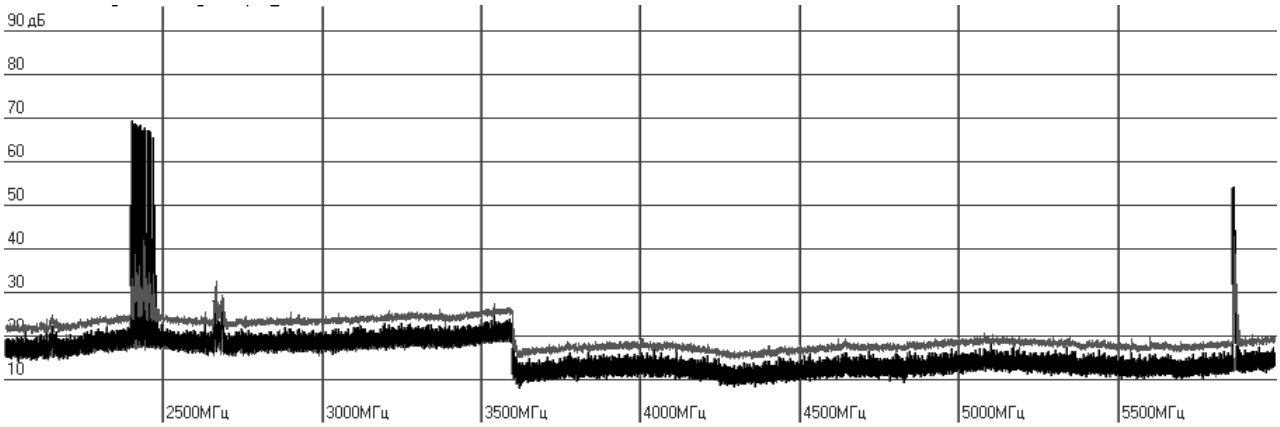
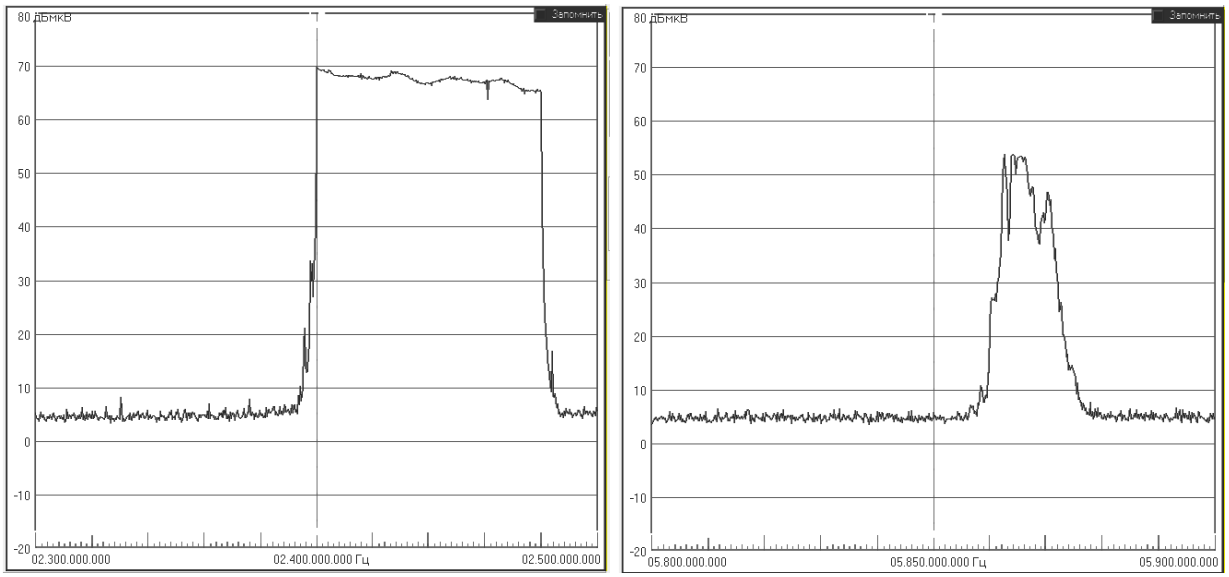


Рис. 3. – Спектральная панорама

Представленная на рисунке 3 радиочастотная панорама имеет 3 выраженных области информативного сигнала с центрами в 2,45, 2,6 и

5,87 ГГц. Две из них соответствует ожидаемым частотам – канал управления работает на частотах 2,4 ГГц, а канал видеопередачи – на 5,8 ГГц. Дополнительно была зафиксирована относительно слабая полоса излучения в районе 2,6 ГГц, назначение которой однозначно не идентифицировано, в т.ч. отсутствует в документации на контроллер.

Занимаемый спектр частот в области 2,45 и 5,87 ГГц, представлен на рисунке 4.



а) б)

Рис. 4. – Спектры частот в области 2,45 ГГц (а) и 5,87 ГГц (б)

Частота видеопередатчика 5,87 ГГц (рис.4б) выявлена однозначно: спектр содержит широкополосный сигнал с полосой порядка 20–40 МГц, характерной для аналогового видеосигнала. Этот канал, как ожидалось, не имел каких-либо признаков шифрования: несущую видеосигнала можно принять стандартным радиоприемником на обнаруженной частоте, что подтвердилось в ходе проведенных экспериментов.

Спектрограмма сигналов управления с центром в 2,45 ГГц имела вид последовательности коротких «пакетных» посылок с периодическим характером, разбросанных по подчастотам внутри диапазона. Представленный на рис.4а спектр частот является результатом измерений в

режиме максимального накопления за, примерно, 30 секунд. Пример измеренных сигналов управления представлен в следующей таблице.

Таблица № 1

Параметры измеренных сигналов с центром 2,45 ГГц

F, МГц	Сигнал, дБмкВ	Шум, дБмкВ	Ширина, кГц
2398,6500	28,16	5,76	300
2398,8600	28,71	5,54	300
…	…	…	…
2450,1700	30,31	5,80	240
2450,4150	36,78	6,48	310
…	…	…	…
2472,4600	34,76	5,79	300
2472,6400	28,22	5,40	300

В представленной таблице продемонстрирована небольшая часть измеренных сигналов передачи команд управления, число которых, в ходе исследования, составило более 130 единиц. Можно отметить, что варьирование уровня сигнала в достаточно широких пределах (от 28,16 дБмкВ до 36,78 дБмкВ) связано в первую очередь с чрезвычайно быстрой и псевдослучайной перестройкой рабочей частоты в технологии FHSS, что не позволяло автоматизированной системе, в ряде случае, полностью зафиксировать пик сигнала в окне просмотра. Средний уровень сигнала составил порядка 31,16 дБмкВ.

Следующий этап исследования предполагал реализацию перехвата управляющего сигнала и его воспроизведение с помощью программно определяемого радиоприёмника. Согласно тактико-техническим характеристикам устройства, полоса пропускания составляет 20 МГц, в то время как измеренный спектр сигнала управления БВС занимает полосу около 74 МГц. Для проведения экспериментальных исследований перехват осуществлялся в БЭК на различных участках спектра с полосой в 5,5 МГц.

Прямое декодирование сигнала протокола ELRS не осуществлялось. В память устройства сохранялись «сырые» данные радиоэфира. Поскольку протокол ELRS не использует шифрование, произвести оцифровку

полученных данных возможно программно-аппаратными средствами самого приемного устройства, но не целесообразно, в рамках проведения экспериментального исследования.

Используя встроенный в приемное устройство инструменты все перехваченные записи воспроизводились в цикличном режиме. Пример визуализации сигнала представлен в форме «водопада» на рисунке 5: каждая линия показывает спектр сигнала, его частоты и амплитуду.

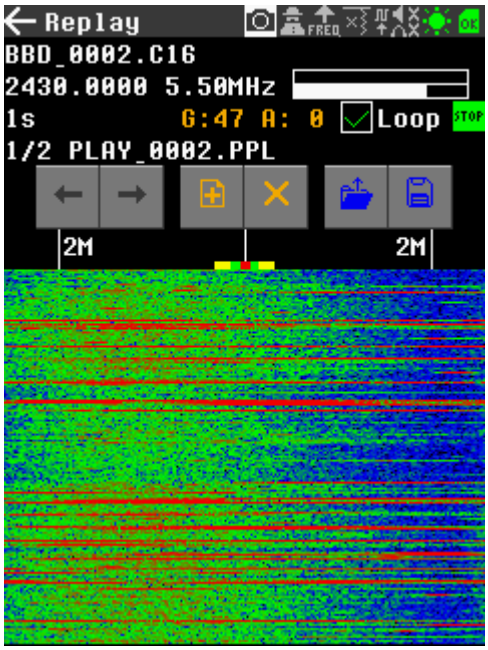


Рис. 5. – Визуализация воспроизведенного сигнала

Рисунок содержит пример визуализации воспроизведения перехваченного ранее сигнала на частоте 2,430 МГц с полосой пропускания 5,5 МГц. Моделирование реализации угрозы активного перехвата и повторения сигнала не вызвало отклика со стороны БВС. Это свидетельствует о том, что канал передачи команд управления действительно устойчив к перехвату за счет использования технологии FHSS, реализованной в протоколе ELRS и повтор старых пакетов не принимался дроном.

Отсюда следует вывод, что технология FHSS, применяемая в ELRS, значительно затрудняет анализ сигналов управления, в том числе со стороны злоумышленников. Псевдослучайная перестройка рабочей частоты, в

совокупности с использованием идентификационной фразы, известной только отправителю и получателю сигнала, повышает защищенность канала управления БВС, снижает вероятность реализации большинства видов атак, таких как перехват и спуфинг. Вместе с тем, риски потери синхронизации между БВС и станцией управления, а также потери управления, вызванные подавлением и физическим вмешательством, остаются весьма критичными для обеспечения безопасного использования дронов.

Кроме того, согласно банку данных угроз безопасности информации ФСТЭК России, в протоколе ELRS имеется уязвимость кода высокого уровня опасности, позволяющая нарушителю, действующему удалённо, перехватить значение идентифицирующей фразы и получить полный контроль над устройством [10]. Согласно исследованию специалистов [11], на стадии сопряжения БВС и станции управления (пульта) злоумышленник способен извлечь часть идентификационной фразы. Блок-схема алгоритма перехвата части идентификационной фразы показана ниже.

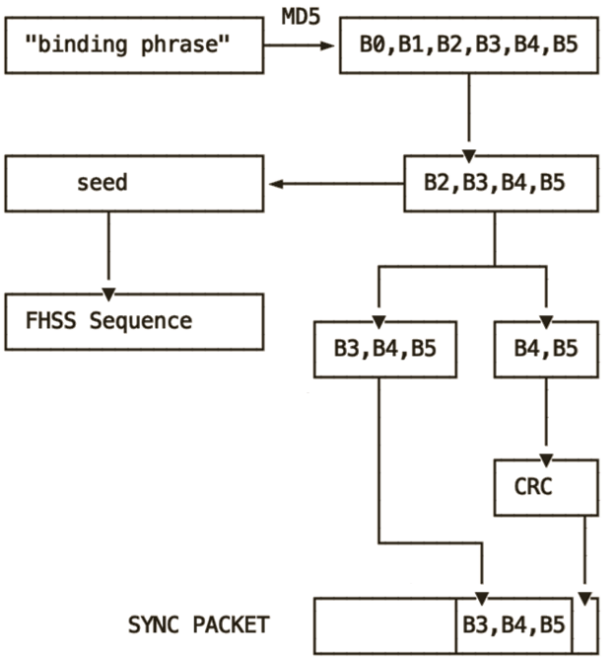


Рис. 6. – Блок-схема алгоритма перехвата части идентификационной фразы

Связующая фраза проходит через алгоритм криптографического хеширования MD5, в результате чего получается уникальная последовательность байтов. Первые 6 байтов этой последовательности сохраняются в виде общего идентификатора между приемником и передатчиком. Последние четыре байта идентификатора используются в качестве начального значения для генерации случайной последовательности частотно-модулированного широкополосного сигнала. И передатчик, и приёмник синхронно переключаются между частотами в последовательности FHSS. Пакет синхронизации отправляется с передатчика на приёмник в начале соединения и через равные промежутки времени в последовательности FHSS. Злоумышленник, получив доступ к открыто передаваемым в радиоэфире четырём байтам, может провести анализ и перебор для определения оставшейся ее части. Как только полный идентификатор будет найден, злоумышленник сможет использовать свой передатчик для управления БВС с установленным внутри приемником.

В настоящее время данная уязвимость не устранена и является весьма актуальной, в связи с чем ФСТЭК России предлагает возможные компенсирующие меры по ее устранению [10], одна из которых предполагает использование более безопасных алгоритмов или настроить существующий алгоритм для обхода повторяющихся последовательностей.

Таким образом, в целях обеспечения безопасного управления БВС актуальна разработка новых эффективных алгоритмов защиты каналов взаимодействия беспилотников со станцией управления от перехвата. Наиболее перспективным способом защиты является интеграция криптографических алгоритмов шифрования сигналов управления путем модифицирования открытого исходного кода протокола ELRS или создания собственных программно-аппаратных модулей, внедренных в прошивку БВС [6]. К примеру, для безопасной передачи идентифицирующей фразы

актуально использовать ассиметричное шифрование на основе попарной выработки открытого и закрытого ключей, что позволит нейтрализовать обнаруженную в ELRS уязвимость по перехвату.

Заключение

Проведённое исследование позволило комплексно оценить уровень защищённости канала управления беспилотного воздушного судна на базе протокола ELRS от несанкционированного перехвата и вмешательства.

Экспериментальные измерения в безэховой камере выявили ожидаемые рабочие частоты каналов управления (2,45 ГГц) и видеопередачи (5,87 ГГц), а также показали возможность перехвата сигнала управления, в виду отсутствия шифрования.

Технология частотного расширения спектра с прыжками по частотам FHSS, реализованная в ELRS, демонстрирует высокую эффективность в противодействии пассивным методам перехвата. Вместе с тем, известная критическая уязвимость протокола ELRS позволяет практически беспрепятственно перехватить управление БВС.

Таким образом, несмотря на эффективность FHSS в защите от простых методов перехвата, существующие уязвимости ELRS требуют незамедлительной модернизации. Реализация предложенных мер позволит существенно повысить безопасность эксплуатации БВС, используемых в деятельности органов внутренних дел, и минимизировать риски несанкционированного вмешательства в их управление.

Литература

1. Кавелин А.С., Тютина А.Д., Нуриев В.Э. Использование квадрокоптеров для обследования объектов // Инженерный вестник Дона, 2019, №7 URL: ivdon.ru/ru/magazine/archive/N7y2019/6108/.

2. Мельникова Е.С., Габова В.В., Чураков А.А., Недожегина И.В. Защитные вантовые конструкции: эффективность и перспективы противодействия БПЛА // Инженерный вестник Дона, 2025, №7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10240/.

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

4. Жилин Р.А., Петренко А.А. Особенности применения беспилотных воздушных судов в деятельности органов внутренних дел Российской Федерации // Охрана, безопасность, связь. 2024. № 9-3. С. 243-245.

5. Смык Е.И., Комаров В.В., Качурина И.Б. Некоторые особенности формирования у сотрудников органов внутренних дел навыков управления беспилотным воздушным судном при решении оперативно-служебных задач Вестник экономической безопасности. 2024. № 2. С. 259-262.

6. Минаев В.А., Бондарь К.М., Дунин В.С., Толпыгин А.С., Федорович В.Ю. Искусственный интеллект: противодействие киберпреступности: моногр. – Хабаровск: РИО ДВЮИ МВД России имени И.Ф. Шилова, 2025. 256 с.

7. Aouladhadj D, Kpre E, Deniau V, Kharchouf A, Gransart C, Gaquière C. Drone Detection and Tracking Using RF Identification Signals. Sensors. 2023; 23(17):7650.

8. Yang H., Liu Y., Li X. et al. Physical layer security and covert communication in UAV-ISAC networks: A comprehensive survey. J. King Saud Univ. Comput. Inf. Sci. 37, 312 (2025).

9. Ullah H., Faisal M., Ali I. (2025). Enhancing UAV Security Through Quantum Cryptography: Current Strategies and Future Pathways. In: Goyal, S.B., Kumar, V., Islam, S.M.N., Ghai, D. (eds) Quantum Computing, Cyber Security and Cryptography. Springer, Singapore.

10. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Банк данных угроз безопасности информации. Уязвимость системы радио управления ExpressLRS (BDU:2022-04040). — URL: bdu.fstec.ru/vul/2022-04040 (дата обращения: 10.11.2025).

11. NCC Group. Technical Advisory: ExpressLRS Vulnerabilities Allow for Hijack of Control Link / NCC Group Trustworthy Technology Lab. — Опубликовано: 30.06.2022. — URL: nccgroup.com/research-blog/technical-advisory-expresslrs-vulnerabilities-allow-for-hijack-of-control-link/ (дата обращения: 10.11.2025).

References

1. Kavelin A.S., Tyutina A.D., Nuriev V.E. Inzhenernyj vestnik Dona, 2019, №7. URL: ivdon.ru/ru/magazine/archive/N7y2019/6108/.

2. Mel'nikova E.S., Gabova V.V., Churakov A.A., Nedozhegina I.V. Inzhenernyj vestnik Dona, 2025, №7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10240/.

3. Minaev V.A., Tolpygin A.S. Informatsiya i bezopasnost'. 2024. T.27. №2. p.177-184.

4. Zhilin R.A., Petrenko A.A. Okhrana, bezopasnost', svyaz'. 2024. № 9-3. pp. 243-245.

5. Smyk E.I., Komarov V.V., Kachurina I.B. Vestnik ekonomicheskoy bezopasnosti. 2024. № 2. pp. 259-262.

6. Minaev V.A., Bondar' K.M., Dunin V.S., Tolpygin A.S., Fedorovich V.Yu. Iskusstvennyy intellekt: protivodeystvie kiberprestupnosti [Artificial intelligence: countering cybercrime]: monogr. Khabarovsk: RIO DVYuI MVD Rossii imeni I.F. Shilova, 2025. 256 p.

7. Aouladhadj D, Kpre E, Deniau V, Kharchouf A, Gransart C, Gaquière C. Sensors. 2023; 23(17):7650.

8. Yang H., Liu Y., Li X. et al. Physical layer security and covert communication in UAV-ISAC networks: A comprehensive survey. J. King Saud Univ. Comput. Inf. Sci. 37, 312 (2025).

9. Ullah H., Faisal M., Ali I. (2025). Enhancing UAV Security Through Quantum Cryptography: Current Strategies and Future Pathways. In: Goyal, S.B., Kumar, V., Islam, S.M.N., Ghai, D. (eds) Quantum Computing, Cyber Security and Cryptography. Springer, Singapore.

10. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii). Bank dannykh ugroz bezopasnosti informatsii. Uyazvimost' sistemy radio upravleniya ExpressLRS (BDU: 2022 04040) [Federal Service for Technical and Export Control (FSTEC of Russia). A database of information security threats. Vulnerability of the ExpressLRS radio control system]. URL: bdu.fstec.ru/vul/2022-04040 (date assessed: 10.11.2025).

11. NCC Group. Technical Advisory: ExpressLRS Vulnerabilities Allow for Hijack of Control Link. NCC Group Trustworthy Technology Lab. Opublikovano: 30.06.2022. URL: nccgroup.com/research-blog/technical-advisory-expresslrs-vulnerabilities-allow-for-hijack-of-control-link/ (date assessed: 10.11.2025).

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 8.11.2025

Дата публикации: 16.12.2025