Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2024-14-2-40-59

УДК 004.056.53

Методы противодействия атакам и организации выбора средств защиты каналов при управлении авиационными робототехническими устройствами

А. В. Хмелевская[1], И. Г. Бабанин[1] ✉, А. Е. Севрюков[1], А. И. Николаенко, Е. Ю. Бабанина, А. А. Севрюков[2]

[1] Юго-Западный государственный университет
ул. 50 лет Октября, д. 94, г. Курск 305000, Российская Федерация

[2] Общество с ограниченной ответственностью «Эдвансед Трансформейшн Консалтинг»
ул. Большая Новодмитровская, д. 14/7, г. Москва 127015, Российская Федерация

✉ e-mail: babanin_ivan@bk.ru

Резюме

Цель исследования *– выявление организационных и технических методов противодействия атакам на командно-телеметрические линии передачи данных между авиационными робототехническими устройствами и наземными пунктами управления, а также формирование комплексной защиты информации рассматриваемых каналов связи.*

Методы. *В научной статье обоснованы методы смягчения и противодействия атакам на физическом уровне модели взаимодействия открытых систем ISO/OSI для организации связи по протоколу MAVLINK с целью управления авиационными робототехническими устройствами (помехоустойчивое кодирование с высокой скоростью кода (на примере наиболее распространенного кода – Витерби), метод расширения спектра скачкообразной перестройкой частоты (FHSS), метод передачи с расширенным спектром прямой последовательности (DSSS), технология множественного входа и множественного выхода (MIMO)). Обозначен метод организации выбора средств защиты и противодействия при управлении авиационными робототехническими устройствами, который заключается в оценке рисков и последствий реализации уязвимостей с целью внедрения контрмер там и в таком количестве, чтобы они имели наибольшую пользу.*

Результаты. *В статье рассмотрены основные возможности по преднамеренному помеховому воздействию на каналы управления и передачи данных потребительских авиационных робототехнических устройств, рассмотрен алгоритм оценки риски «уход с маршрута»; приведен вариант оценки риска применительно к риску схода летательного аппарата с маршрута с указанием названия атаки, ее вероятности, воздействия и возникающего риска, а также приемлемость этого риска и рекомендации относительно срочности его смягчения; представлены рекомендации контрмер в соответствии с приемлемостью вероятности и воздействия; описано соотношение риска и контрмер, применяемых для снижения несанкционированного воздействия, в соответствии с весовыми коэффициентами.*

Заключение. *В научной статье рассмотрены основные методы противодействия атакам и несанкционированного доступа при управлении автономными робототехническими устройствами. Рассмотрены коэффициенты рисков атак и предпринимаемых контрмер.*

Ключевые слова: *авиационное робототехническое устройство; криптозащита информации; каналы управления; несанкционированный доступ; оценка рисков.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Методы противодействия атакам и организации выбора средств защиты каналов при управлении авиационными робототехническими устройствами / А. В. Хмелевская, И. Г. Бабанин, А. Е. Севрюков, А. И. Николаенко, Е. Ю. Бабанина, А. А. Севрюков // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2023. Т. 14, № 2. С. 40–59. https://doi.org/10.21869/ 2223-1536-2024-14-2-40-59

Поступила в редакцию 07.04.2024 *Подписана в печать 03.05.2024* *Опубликована 28.06.2024*

Methods of countering attacks and organizing the choice of channel protection tools when controlling aviation robotic devices

Alena V. Khmelevskaya[1], Ivan G. Babanin[1] ✉, Aleksandr E. Sevryukov[1], Anton I. Nikolaenko[1], Ekaterina Y. Babanina[1], Anton A. Sevryukov[2]

[1] Southwest State University
50 Let Oktyabrya Str. 94, Kursk 305040, Russian Federation

[2] Limited Liability Company "Advanced Transformation Consulting"
14/7 Bolshaya Novodmitrovskaya Str., Moscow 127015, Russian Federation

✉ e-mail: babanin_ivan@bk.ru

Abstract

The purpose of the research *is identification of organizational and technical methods of countering attacks on command and telemetry data transmission lines between aviation robotic devices and ground control points, as well as the formation of comprehensive information protection of the communication channels under consideration.*

Methods. *The scientific article substantiates methods for mitigating and countering attacks at the physical level of the ISO/OSI open systems interaction model for organizing communication using the MAVLINK protocol for the purpose of controlling aviation robotic devices (noise-resistant coding with a high code rate (using the example of the most common code - Viterbi), extension method Frequency Hopping Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Multiple Input Multiple Output (MIMO) technology). A method for organizing the selection of protection and countermeasures when controlling aviation robotic devices is outlined, which consists of assessing the risks and consequences of the implementation of vulnerabilities in order to introduce countermeasures there and in such quantities that they have the greatest benefit.*

Results. *The article discusses the main possibilities for intentional interference on the control and data transmission channels of consumer aviation robotic devices, an algorithm for assessing the risk of "leaving the route" is considered; a risk assessment option is provided in relation to the risk of an aircraft going off route, indicating the name of the attack, its likelihood, impact and resulting risk, as well as the acceptability of this risk and recommendations regarding the urgency of mitigating it; recommendations for countermeasures are presented in accordance with the acceptability of likelihood and impact; describes the relationship between risk and countermeasures used to reduce unauthorized exposure, in accordance with weighting coefficients.*

Conclusion. *The scientific article discusses the main methods of countering attacks and unauthorized access when controlling autonomous robotic devices. The risk coefficients of attacks and countermeasures taken are considered.*

Keywords: *aviation robotic device; cryptographic information protection; control channels; unauthorized access; risk assessment.*

Conflict of interest: *The Authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Khmelevskaya A.V., Babanin I.G., Sevryukov A.E., Nikolaenko A.I., Babanina E.Y., Sevryukov A.A. Methods of countering attacks and organizing the choice of channel protection tools when controlling aviation robotic devices. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2024;14(2):40–59. (In Russ.) https://doi.org/10.21869/2223-1536-2024-14-2-40-59.

Received 07.04.2024 *Accepted 03.05.2024* *Published 28.06.2024*

***

Введение

На сегодняшний день применение авиационных робототехнических устройств позволяет решить наиболее острые и актуальные проблемы. В их числе и экономические, и экологические, и другие потребности, с которыми связано большинство отраслей во всем мире. Применение авиационных робототехнических устройств позволяет производить осмотр магистральных линий электропередач, производить мониторинг местности, осуществлять разведку и в целом выполнять ряд важнейших задач. Однако на данный момент остро стоит вопрос о стандартизации данной отросли, поскольку существующие стандарты ориентируются в основном лишь на проблематике безопасности полетов.

Существующий на данный момент Международный стандарт ISO 21384-3:2019(E) предписывает внедрение в качестве основной системы практику управления безопасностью полетов вне зависимости от подвида применяемых авиационных робототехнических устройств. Данное направление подразумевает использование всех существующих на сегодняшний день мер обеспечения информационной безопасности в полном контексте использования летательного аппарата [1].

В основе работы многих современных авиационных робототехнических устройств лежит принцип обмена информацией с наземными пунктами управления (НПУ), который во многих случаях осуществляется в соответствии с принципами протокола MAVLink. Однако при этом выявляется существенный недостаток использования данного протокола – вопрос обеспечения защиты передаваемой информации, поскольку MAVLink не предполагает использования никакой защиты передаваемых данных, что влечет за собой риски перехвата и взлома передаваемых данных. Данный протокол не предполагает использования методов аутентификации и идентификации, т. е., по сути, связь между авиационным робототехническим устройством и НПУ осуществляется по незащищенному и незашифрованному каналу связи. Таким образом, высока вероятность несанкционированного воздействия третьих лиц на полетное задание авиационного робототехнического устройства и в целом его поведение, а также и перехват заданий для робототехнического устройства. Альтернативой применению

MAVLink является использование его модернизированной версии – протокола MAVSec, который обладает механизмами криптозащиты [2]. Особенно остро стоит вопрос о несанкционированном воздействии на программу выполнения заданий во время полета авиационного робототехнического устройства. Например, создается угроза возникновения уязвимости, суть которой заключается в возможности вставки вредоносного кода в алгоритм работы авиационного робототехнического устройства непосредственно во время полета (данное воздействие может иметь самые различные последствия) от некорректного поведения аппарата до полной потери авиационного робототехнического устройства. Для смягчения угроз от «площадных» помех и эффективного противодействия им программа, контролирующая полет, может использовать систему, в основе которой лежит принцип обнаружения вторжений (IDS). Эта система, как правило, представляет собой программно-аппаратное обеспечение, которое отслеживает аномалии и отклонения в системе [3].

IDS для предотвращения неправильного использования работает с заранее определенными сигнатурами атак, которые нацелены на уязвимые точки системы безопасности. Эти сигнатуры хорошо известны и используются в качестве шаблонов для сравнения.

IDS для обнаружения аномалий сравнивает текущую производительность системы с ее обычной производительностью, сформированной на основе статистики. Если система показывает отклонения от своей обычной производительности, IDS регистрирует это поведение. IDS также идентифицирует входящий трафик, определяя, нуждается ли он в защите, и использует для этого три различных типа информации. К данным типам относятся:

– информация, имеющая долгосрочных характер;

– информация, включающая данные о текущей конфигурации системы;

– информация текущего аудита авиационного робототехнического устройства.

К первому типу информации, а именно к долгосрочной информации, следует отнести создание базы данных методов обнаружения атак. Ко второму типу, соответственно, следует отнести информацию по текущему состоянию системы. Аналогично конфигурационной информации, информация аудита соответственно также отражает состояние системы в данный момент, при этом систематизируя данные аудита и текущее состояние системы, возможно, определение, обнаружены ли признаки несанкционированного вторжения или нет. Далее соответственно предпринимаются действия для возврата системы авиационного робототехнического устройства в наиболее безопасное в данной ситуации состояние.

Оптимальное управление правилами осуществляется с использованием критериев приоритета. В основе каждого правила лежит принцип формирования

не на одном лишь состоянии авиационного робототехнического устройства, а на совокупности состояний, которые предполагают наличие как состояний с безопасным и нормальным поведением, так и с состояниями, которые могут возникнуть в результате несанкционированного воздействия на робототехническое устройство.

Таким образом, формируемые правила имеют в своем составе целый набор состояний, которые указывают, находится ли аппарат в безопасном режиме или подвержен несанкционированному воздействию, которое не описано в данном правиле.

Материалы и методы

Преднамеренное помеховое воздействие на каналы управления и передачи данных потребительских авиационных устройств не имеет широкого распространения среди злоумышленников и малоэффективно в реальных ситуациях из-за ряда особенностей реализации такого воздействия, а также благодаря существующим методам повышения помехозащищённости каналов.

К особенностям реализации воздействий относятся:

– преднамеренное воздействие осуществимо лишь при условии соблюдения электромагнитной доступности авиационного робототехнического устройства [4];

– в режиме «радиомолчания» или при автономном движении робототехнического устройства по заранее запрограммированной траектории приём и анализ радиоэлектронного взаимодействия устройства крайне затруднён или невозможен;

– энергетическая эффективность средств воздействия убывает пропорционально квадрату расстояния;

– «площадные» заградительные помехи эффективно подавляют несколько каналов управления и навигации. Однако их использование с БПЛА, которые в своем рабочем состоянии используют широкополосные сигналы и сигналы с псевдослучайной перестройкой рабочей частоты, может быть менее эффективным из-за снижения энергетической эффективности [5];

– помехи, основной замысел которых заключается в частотной и структурной идентификации сигналов, имеющие наибольший эффект в целях несанкционированного воздействия на авиационное робототехническое устройство, которые имеют своей целью искажение полетного задания, в т. ч. отправка фиктивных команд для нарушения полетного задания авиационного устройства или режима работы в целом, требуют либо изначального вскрытия структуры сигналов и формата команд авиационного робототехнического устройства, либо заблаговременного перехвата баз данных соответствующих команд, используемых при работе с авиационным аппаратом [6];

– характер движения авиационного устройства существенно влияет на эффективность радиоэлектронного воздействия со стороны статичного средства

злоумышленника (складки местности, здания, полёт на низкой высоте);

– ограниченность в энергетических ресурсах и ресурсах времени воздействия на летательных аппарат, полёт которого, в свою очередь, ограничен рамками сессии (порядка 40–50 мин).

К существующим методам помехозащищённости каналов управления и передачи относятся нижеприведённые.

Применение помехоустойчивого кодирования с высокой скоростью кода. Для решения вопроса оценка вклада помехоустойчивого кодирования в проблему, связанную с улучшением криптозащищенности радиолиний связи с авиационным аппаратом, проводилась с использованием анализа значения вероятности ошибки на бит на входе (*Pb in Vit*) и на выходе декодера Витерби (*Pb out Vit*). Данные значения для райсовской и рэлеевской радиолиний для кодовых скоростей R = 1/2, 2/3, 3/4, 5/6, 7/8 для сигнала КАМ-64 представлены ниже (рис. 1).

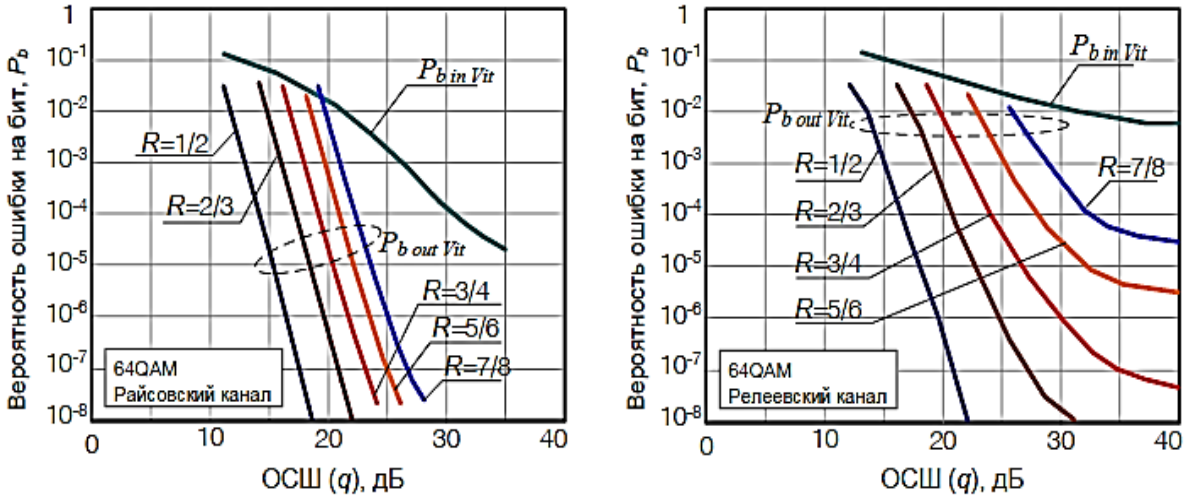

Рис. 1. Значения вероятности возникновения битовой ошибки от скорости кодирования [7]

Fig. 1. Bit error probability as a function of encoding speed [7]

Применение метода расширения спектра скачкообразной перестройкой частоты (FHSS) основано на периодическом изменении несущей частоты сигнала. Хотя в любой данный момент передатчик работает как простой узкополосный передатчик, по прошествии заданного времени частота изменяется, вызывая перемещение несущего информацию сигнала. Несущая частота перемещается дискретными шагами, или скачками, в пределах заданной полосы частот, и конечный результат состоит в том, что в течение определенного периода времени передача распространяется по широкой полосе частот или спектру. Если существует вероятность того, что узкополосный передатчик создаст помехи, то с течением времени этот узкополосный передатчик остается на фиксированной частоте, а передача полезного сигнала перемещается на другую несущую частоту псевдослучайным образом. Для создания широкополосной

помехи, способной вызвать недопустимое количество битовых ошибок для канала передачи БПЛА, требуется большие ресурсы энергии.

Метод передачи с расширенным спектром прямой последовательности (DSSS) – это принципиально другой метод, используемый в ситуациях, подверженных помехам. Он использует схему для свертывания потока данных с помощью кода расширения. Метод противодействует помехам, смешивая сигнал данных с PN кодом, шумоподобной последовательностью битов или элементарных посылок со значениями 0 и 1. Результирующая ширина полосы сигнала становится намного больше («расширенный спектр»). Приемная система применяет тот же PN код к принятому сигналу для извлечения / декодирования информации. Суть этого метода расширения заключается в том, что несущая частота остается фиксированной, в то время как передаваемый сигнал расширяется. Передатчик работает не с битовой скоростью цифровой информации, а с более высокой битовой скоростью, связанной с кодированным сигналом. Это приводит к увеличению энергии бокового лепестка по мере увеличения размера расширяющегося PN кода. Чем больше битов добавляется к коду расширения, тем больше энергии передается в боковые лепестки, тем самым уменьшая амплитуду любого отдельного лепестка. При определённом коде расширения можно понизить энергию в любом одном боковом лепестке до уровня ниже минимального уровня шума анализатора спектра.

Технология множественного входа и множественного выхода (MIMO) относится к технологии беспроводной связи, которая передает сигналы через несколько антенн на передающей стороне и принимает сигналы через несколько антенн на принимающей стороне. MIMO в сочетании с технологией мультиплексирования с ортогональным частотным разделением каналов и пространственно-временное кодирование могут реализовать пространственное разнесение, временное разнесение и частотное разнесение, тем самым реализуя антиинтерференцию в пространственной, временной и частотной области [8].

Риски нежелательного воздействия на летательный аппарат могут возникать на каждом этапе полётной миссии. Риски, возникающие во время полета, обычно находятся в центре внимания из-за возникающей угрозы безопасности, однако риски до полёта или после полёта не менее важны.

Предполетные риски включают приобретение, сборку и настройку аппаратного и программного обеспечения авиационного робототехнического устройства, а также применение различных веб-приложений, которые представляют собой угрозы как безопасности, так и конфиденциальности.

Риски после полета включают обработку данных и соответствующую инфраструктуру хранения, которая может угрожать конфиденциальности.

Систематизация рабочего процесса помогает определить и спланировать миссию. Следовательно, разработка такого метода организации рабочего процесса может способствовать снижению технического риска ещё до его реализации извне [9].

Стандарты, специфичные для предметной области, часто не учитывают сдвиг в сторону программных возможностей или явно не подчеркивают соответствующие риски информационной безопасности, возникающие при реализации таких функций в программном обеспечении. Зачастую стандарты не содержат ссылок на количественные процедуры, которые могут обеспечить желаемые возможности поддержки принятия решений.

Существует необходимость в простых количественных процедурах для оценки рисков, сравнения эффективности мер противодействия и передачи связанных результатов.

Основная идея организации выбора методов защиты, противодействия и смягчения последствий заключаются в следующем: оценка рисков и последствий реализации уязвимостей для внедрения контрмер там и в таком количестве, чтобы они имели наибольшую пользу.

Концептуальный подход к количественной оценке риска летательного аппарат и объективная стратегия снижения риска посредством усовершенствования технологии или контрмер графически представлены ниже (рис. 2).

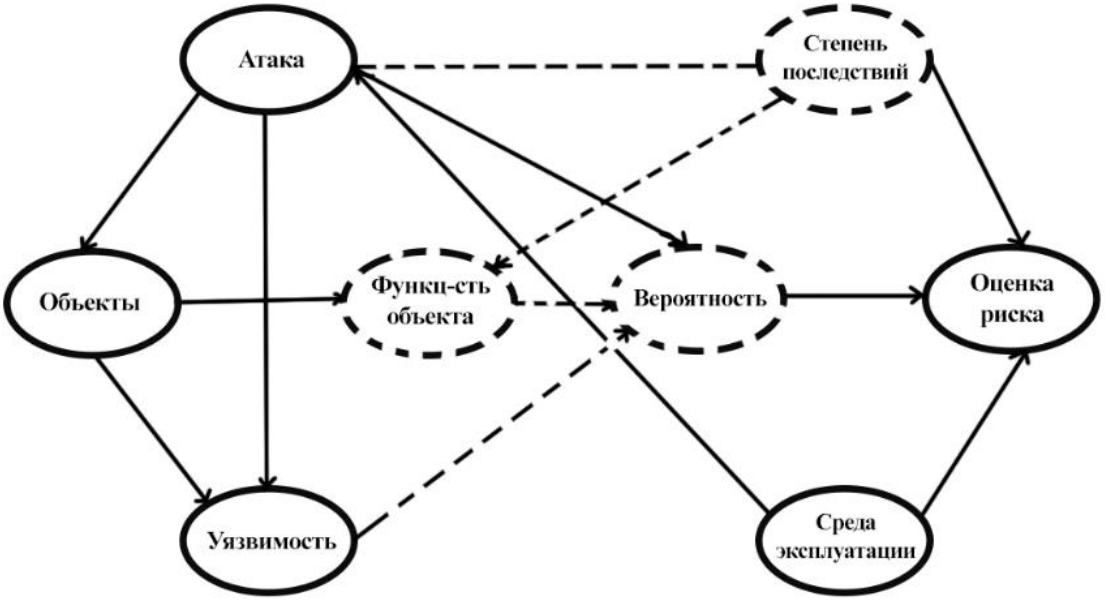

Рис. 2. Схема количественной оценки рисков воздействия на летательный аппарат [10]

Fig. 2. A scheme for quantifying the risks of exposure to an aircraft [10]

На рисунке 2 присутствует восемь узлов, а также соответствующие отношения между ними. Объекты функционала БПЛА предоставляют его функциональные возможности. Однако эти же объекты функционала также обладают уязвимостями. Атаки нацелены на объекты функционала через его уязвимости. Атаки происходят в среде эксплуатации и успешны с определенной вероятностью,

приводя к последствиям определенной степени серьезности. Наконец среда эксплуатации, вероятность возникновения и степень последствий вносят вклад в оценку риска [11].

Вероятность возникновения воздействия на объект функционала и степень (тяжесть) последствий служат основой для предварительных формулировок количественной оценки риска.

Организация выбора методов и средств управления рисками требует выявления рисков и их потенциальных последствий. Только тогда можно определить стратегию снижения этих рисков.

На рисунке 3 проиллюстрирована схема алгоритма (полетное задание – оценка рисков при выполнении – решение возникших аспектов – выполнение / невыполнение задания) оценки риска «Уход с маршрута», когда одна из нескольких атак заставляет авиационное устройство нарушить полётную миссию [12].

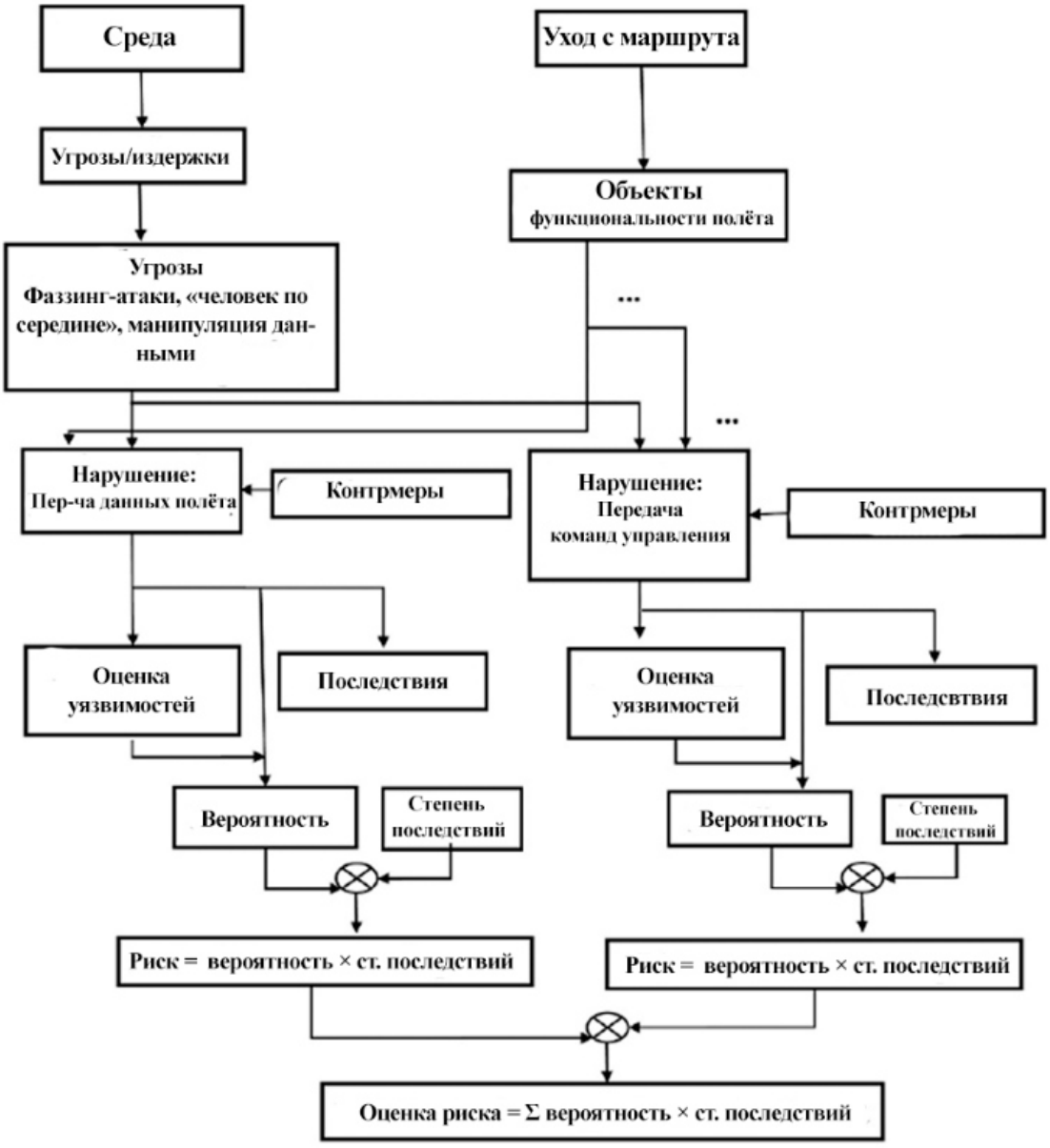

Рис. 3. Алгоритм оценки риски «Уход с маршрута»

Fig. 3. Risk assessment algorithm "Leaving the route"

Контрмеры различной сложности и стоимости могут снизить уязвимость и последствия атаки, что может снизить вероятность успеха атаки, а также ее воздействие и соответствующую серьезность. Традиционные модели риска определяют риск как произведение вероятности и времени воздействия [13].

Поскольку точные вероятности рисков трудно определить и вычислить, вводится пятиуровневая матрица вероятностей рисков и их словесное кодирование (часто (Д), случайное (Г), маловероятно (В), практически невероятно (Б) и крайне маловероятное (А)). Таким образом, при таком подходе оценка упрощается до категорий, чтобы способствовать принятию решения и его имплементации (табл. 1).

Таблица 1. Пятиуровневая система классификации и кодирования

Table 1. Five-level classification and coding system

Степень последствий	5	5А	5Б	5В	5Г	5Д
	4	4А	4Б	4В	4Г	4Д
	3	3А	3Б	3В	3Г	3Д
	2	2А	2Б	2В	2Г	2Д
	1	1А	1Б	1В	1Г	1Д
		А	Б	В	Г	Д
		Вероятность				

Аналогичным образом по пятиуровневой системе классифицируется и кодируется степень последствий (чрезвычайно высокий уровень (5), высокий (4), средний (3), низкий (2) и чрезвычайно низкий (1)). Однако, как указывалось ранее, это также может быть скорректировано в соответствии с потребностью и практикой взаимодействия с летательным аппаратом [14].

Предполагая, что риски нарушения функционала являются взаимоисключающими, можно суммировать оценки рисков для каждого нарушения, чтобы получить Риск («Уход с маршрута») = Σ «Вероятность» × «Степень воздействия», включая каждую угрозу, специфичную для этого риска [15].

В таблице 2 приведены пример оценки риска применительно к риску схода авиационного робототехнического устройства с маршрута с указанием названия атаки, ее вероятности, воздействия и возникающего риска, а также приемлемость этого риска и рекомендации относительно срочности его смягчения. Вероятность и воздействие зависят от конкретной выполняемой миссии, поэтому для иллюстрации были присвоены условные значения.

В таблице 3 представлены рекомендации в соответствии с приемлемостью вероятности и воздействия.

Таблица 2. Оценки риска применительно к риску схода авиационного робототехнического устройства с маршрута

Table 2. Risk assessments in relation to the risk of an aircraft robotic device going off the route

Атака	«Вероятность»	Степень последствий	Риск	Приемлемость	Рекомендации
«Человек посередине»	3	2	6	Удовлетворительно	Использование лучших практик
Глушение канала связи	3	3	9	Неприемлемо	Требуется немедленное смягчение последствий
Глушение GNSS	3	2	6	Удовлетворительно	Использование лучших практик
Атака повторного воспроизведения	3	5	15	Допустимо	Никаких действий не требуется
Обман сенсоров	3	2	6	Неприемлемо	Требуется немедленное смягчение последствий
Глушение сенсоров	3	2	6	Удовлетворительно	Использование лучших практик

Таблица 3. Рекомендации контрмер [16]

Table 3. Recommendations of countermeasures [16]

Приемлемость	Вероятность и степень последствий	Рекомендации контрмер
Неприемлемо	3-5Г	Требуются немедленные действия по смягчению и эскалации последствий. Следует рассмотреть возможность оперативной остановки
Удовлетворительно	4-5А, 3-5Б,1-5В, 1-2Г	Риск должен быть минимизирован, насколько это практически возможно, при условии соблюдения формального процесса утверждения
Допустимо	1-3А, 1-2Б	Никаких действий не требуется

В таблице 4 на примерах для ясности обобщена информация об атаках, рисках и контрмерах. Коэффициентам присвоены условные значения, так как вероятность ($В_i$), степень последствий ($П_i$), весовой коэффициент контрмеры ($КП_i$) и стоимость имплементации ($К_с$) зависят от выполняемой миссии и могут быть скорректированы в соответствии с потребностью и практикой применения летательного аппарата [17].

Таблица 4. Коэффициенты рисков, атак и контрмер [16]

Table 4. Coefficients of risks, attacks and countermeasures [16]

Атака (A_i)		B_i	$П_i$	Риск	Контрмеры ($К_i$)		$КП_i$	$К_с$
А1	Внедрение ложных данных	3	4	12	К1	Сверка метаданных и актуальных данных	-1	10
А2	Воздействие на сенсоры через оптический поток	3	3	9	К2	Применение алгоритмов проверки легитимности заземляющей поверхности	-1	5
А3	Глушение канала ЛА-НПУ	3	2	6	К3, К4	Измерение мощности сигнала, смена канала	-2	1
А4	Атаки «человек посередине»	3	5	15	К5	Применение защищённых протоколов	-2	5
А5	Глушение GNSS	3	2	6	К6	Применение SoS- и DoA-детекторов	-1	15
А6	Dos-, ARP-атаки	3	1	3	К7	Применение сторожевого таймера, строгая фильтрация данных, защита точки доступа	-2	1
Суммарный коэф. риска				51				

Цель состоит в том, чтобы определить контрмеры (табл. 2), которые снижают риск до приемлемого уровня, для достижения уровня принятия рисков (табл. 3, 4).

Без назначенных контрмер базовый риск схода с маршрута равен

$P_0 = (4 \cdot 3) + (3 \cdot 3) + (3 \cdot 2) + (3 \cdot 5) + + (3 \cdot 2) + (3 \cdot 1) = 51$, в то время как применение контрмеры, например К5, снижает риск до $P(К2) = (4 \cdot 3) + (3 \cdot 3) + (3 \times \times 2) + ((3-2) \cdot 5) + (3 \cdot 2) + (3 \cdot 1) = 45$.

А эффективное соотношение риска и затрат составляет

$$РК2 = \frac{P_0 - РК5}{К_с} = \frac{51-45}{5} = 1,2.$$

Аналогичным образом определяется снижение риска для других контрмер: $P(К1) = 48$, $P(К2) = 48$, $P(К3) = 48$, $P(К4) = 45$, $P(К6) = 48$ и $P(К7) = 45$.

В таблице 5 показано соотношение риска и стоимости всех контрмер [18].

Таблица 5. Соотношение риска и стоимости контрмер

Table 5. The ratio of risk and cost of countermeasures

Контрмера	Соотношение
К5	1,2
К1	0,3
К2	0,6
К3	3
К4	6
К6	0,2
К7	6

И мера К4, и мера К7 имеют одинаковое соотношение. Однако атака А3 имеет большую степень последствий, чем атака А6, поэтому для противодействия А3 выбирается мера К4. Затем соотношения пересчитываются с новым базовым уровнем общего риска 45 [19].

На рисунке 4 показан приведена функциональная зависимость общего риска при выполнении полетного задания от совокупной стоимости контрмер для избежания несанкционированного воздействия [20].

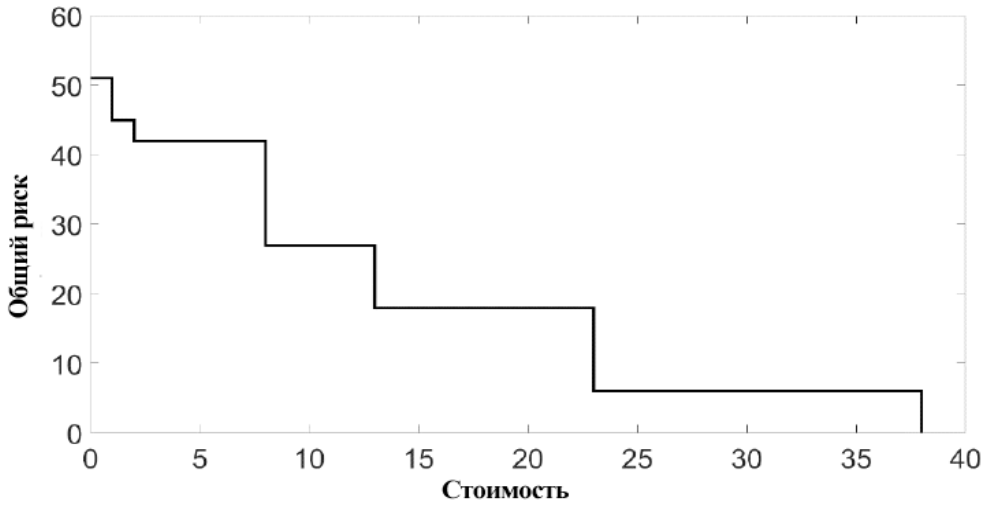

Рис. 4. Функциональная зависимость общего риска при выполнении полетного задания от совокупной стоимости контрмер для избежания несанкционированного воздействия

Fig. 4. Functional dependence of the overall risk in the performance of a flight mission on the total cost of countermeasures to avoid unauthorized exposure

Результаты и их обсуждение

В соответствии с поставленными целями:

– рассмотрены основные возможности по преднамеренному помеховому воздействию на каналы управления и передачи данных потребительских авиационных робототехнических устройств;

– рассмотрен алгоритм оценки риски «уход с маршрута»;

– приведен вариант оценки риска применительно к риску схода летательного аппарата с маршрута с указанием названия атаки, ее вероятности, воздействия и возникающего риска, а также приемлемость этого риска и рекомендации относительно срочности его смягчения;

– представлены рекомендации контрмер в соответствии с приемлемостью вероятности и воздействия;

– описано соотношение риска и контрмер, применяемых для снижения несанкционированного воздействия, в соответствии с весовыми коэффициентами.

Выводы

Рассмотренный подход позволяет лицу, принимающему решение, определить риск, достижимый в рамках определенного бюджета, или затрат, необходимых для достижения желаемого уровня риска. Рассмотренный подход может

служить ориентиром при выборе контрмер, а также при обосновании вспомогательного бюджета для таких контрмер.

По полученным выше данным возможно дальнейшее проектирование системы управления БПЛА с учетом возможных воздействий и применение соответствующих контрмер. В рамках дальнейших исследований планируется к анализу и разработке система управления полетным заданием для БПЛА с учетом применения возможностей по доставке грузов при рассмотрении воздействий, описанных выше.

Список литературы

1. Лисничук А. А. Процедура многокритериального синтеза OFDM-радиосигналов для снижения пик-фактора и повышения структурной скрытности систем передачи информации // Вестник Рязанского радиотехнического университета. 2021. № 77. С. 17–28.

2. Лисничук А. А., Батищев А. В. Двухкритериальный синтез OFDM-сигналов для повышения энергетической эффективности и помехоустойчивости // Вестник Рязанского радиотехнического университета. 2021. № 76. С. 3–16.

3. Лисничук А. А. Многокритериальный синтез радиосигналов с прямым расширением спектра для адаптивных к узкополосным и структурным помехам систем передачи информации // Цифровая обработка сигналов. 2022. № 1. С. 19–23.

4. Многокритериальный подход к выбору процедуры кодирования телеметрических радиосигналов сложных технических объектов / С. Н. Кириллов, А. А. Лисничук, П. С. Писака [и др.] // Вестник Рязанского радиотехнического университета. 2021. № 75. С. 3–14.

5. Способ реализации криптографической защиты каналов для организации связи по протоколу MavLink при управлении автономными БПЛА / А. В. Хмелевская, А. Е. Севрюков, А. А. Севрюков [и др.] // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2022. Т. 12, № 4. С. 122–141.

6. Бабанин И. Г., Мухин И. Е., Коптев Д. С. Методологические основы выбора параметров фильтров частотной селекции с учетом эквивалентных энергетических потерь в радиоприёмных устройствах высокоскоростных радиосистем передачи информации: монография / Юго-Западный государственный университет. Курск, 2020. 136 с.

7. Метод параметрического синтеза систем обеспечения электромагнитного доступа средств радиомониторинга источников радиоизлучения с квадратурной амплитудной модуляцией спутниковых систем связи / И. Г. Бабанин, И. Е. Мухин, Е. Ю. Бабанина, А. В. Хмелевская // Известия Юго-Западного государственного университета.

Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2022. Т. 12, № 4. С. 41–63.

8. Галкин В. А. Основы программно-конфигурируемого радио. М.: Горячая линия – Телеком, 2023. 372 с.

9. Оценка дальности передачи видеоинформации различного качества при мониторинге чрезвычайных ситуаций с беспилотного летательного аппарата / М. Ю. Алемпьев, Д. С. Коптев, В. Г. Довбня, Е. В. Скрипкина // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2023. Т. 13, № 2. С. 31–44.

10. Фокин Г. А. Принципы и технологии цифровой связи на основе программно-конфигурируемого радио: обзор современных тенденций в области создания комплекса подготовки специалистов // Труды учебных заведений связи. 2019. № 5(1). С. 78–94.

11. Прототип приемопередающего оборудования скоростной передачи данных в частотном диапазоне 57–64 ГГц / О. В. Болховская, Г. А. Ермолаев, С. Н. Трушков, А. А. Мальцев // Труды учебных заведений связи. 2023. № 9(2). С. 23–39.

12. Оценка дальности передачи видеоинформации различного качества при мониторинге чрезвычайных ситуаций с беспилотного летательного аппарата / М. Ю. Алемпьев, Д. С. Коптев, В. Г. Довбня, Е. В. Скрипкина // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2023. Т. 13, № 2. С. 31–44.

13. Фокин Г. А. Принципы и технологии цифровой связи на основе программно-конфигурируемого радио: обзор современных тенденций в области создания комплекса подготовки специалистов // Труды учебных заведений связи. 2019. № 5(1). С. 78–94.

14. Липатников В. А., Петренко М. И. Модель самоорганизующейся сети радиосвязи, функционирующей в сложной сигнально-помеховой обстановке // Труды учебных заведений связи. 2023. № 9(2). С. 72–80.

15. Метод и алгоритм автономного планирования траектории полета беспилотного летательного аппарата при мониторинге пожарной обстановки в целях раннего обнаружения источника возгорания / Р. А. Томакова, С. А. Филист, А. Н. Брежнева [и др.] // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2023. Т. 13, № 1. С. 93–110.

16. Кулешова Е. А., Таныгин М. О. Исследование характеристик современных генераторов псевдослучайных последовательностей // Телекоммуникации. 2023. № 7. С. 28–39.

17. Интеллектуальная система обработки изображений, получаемых с беспилотных летательных аппаратов / С. А. Филист, Р. А. Томакова, Н. Г. Нефедов [и др.] // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2022. Т. 12, № 4. С. 64–85.

18. Larin S. N., Ermakova I. M. Integrated assessment of innovative software projects quality: a system of indicators // International Journal of Humanities and Natural Sciences. 2022. N 3-3(66). P. 179–184.

19. Андронов В. Г., Чуев А. А., Князев А. А. Модель параметров отклонений маршрута полёта беспилотных летательных аппаратов от заданной траектории // Известия Юго-Западного государственного университета. 2021. Т. 25, № 4. С. 145–161. https://doi.org/10.21869/2223-1560-2021-25-4-145-161

20. Использование показателей структуры вибросигнала для решения задач диагностики технического состояния ответственных агрегатов современных летательных аппаратов / И. Е. Мухин, С. А. Тяпкин, Д. С. Коптев, Ю. В. Шуклина // Телекоммуникации. 2023. № 6. С. 2–14. https://doi.org/10.31044/1684-2588-2023-0-6-2-14. EDN ZCPQKS

References

1. Lisnichuk A.A. The procedure of multicriteria synthesis of OFDM radio signals to reduce the peak factor and increase the structural secrecy of information transmission systems. *Vestnik Ryazanskogo radiotekhnicheskogo universiteta = Bulletin of the Ryazan Radio Engineering University*. 2021;(77):17–28. (In Russ.)

2. Lisnichuk A.A., Batishchev A.V. Two-criterion synthesis of OFDM signals to increase energy efficiency and noise immunity. *Vestnik Ryazanskogo radiotekhnicheskogo universiteta = Bulletin of the Ryazan Radio Engineering University*. 2021;(76): 3–16. (In Russ.)

3. Lisnichuk A.A. Multicriteria synthesis of radio signals with direct spectrum expansion for information transmission systems adaptive to narrowband and structural interference. *Tsifrovaya obrabotka signalov = Digital Signal Processing*. 2022;(1):19–23. (In Russ.)

4. Kirillov S.N., Lisnichuk A.A., Pisaka P.S., et al. A multi-criteria approach to the choice of the procedure for encoding telemetric radio signals of complex technical objects. *Vestnik Ryazanskogo radiotekhnicheskogo universiteta = Bulletin of the Ryazan Radio Engineering University*. 2021;(75); 3–14. (In Russ.)

5. Khmelevskaya A.V., Sevryukov A.E., Sevryukov A.A., et al. A method for implementing cryptographic protection of channels for organizing communication using the MAVLink protocol when controlling autonomous UAVs. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control,*

Computer Engineering, Information Science. Medical Instruments Engineering. 2022;12(4):122–141. (In Russ.)

6. Babanin I.G., Mukhin I.E., Koptev D.S. Methodological foundations for the selection of parameters of frequency selection filters taking into account equivalent energy losses in radio receivers of high-speed radio information transmission systems. Kursk: Yugo-Zapadnyi gosudarstvennyi universitet; 2020. 136 p. (In Russ.)

7. Babanin I.G., Mukhin I.E., Babanina E.Y., Khmelevskaya A.V. Method of parametric synthesis of electromagnetic access systems for radio monitoring of radio sources with quadrature amplitude modulation of satellite communication systems. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2022;12(4):41–63. (In Russ.)

8. Galkin V.A. Fundamentals of software-configurable radio. Moscow: Goryachaya liniya; 2023. 372 p. (In Russ.)

9. Alempyev M.Y., Koptev D.S., Dovbnya V.G., Skripkina E.V. Evaluation of the transmission range of video information of various quality when monitoring emergency situations from an unmanned aerial vehicle. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2023;3(2):31–44. (In Russ.)

10. Fokin G.A. Principles and technologies of digital communication based on software-configurable radio: an overview of current trends in the field of creating a complex of training specialists. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2019;5(1):78–94. (In Russ.)

11. Bolkhovskaya O.V., Ermolaev G.A., Trushkov S.N., Maltsev A.A. Prototype of high-speed data transmission equipment in the frequency range 57–64 GHz. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2023;9(2):23–39. (In Russ.)

12. Alempyev M.Y., Koptev D.S., Dovbnya V.G., Skripkina E.V. Evaluation of the transmission range of video information of various quality when monitoring emergency situations from an unmanned aerial vehicle. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe*

priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering. 2023; 13(2):31–44. (In Russ.)

13. Fokin G.A. Principles and technologies of digital communication based on software-configurable radio: an overview of current trends in the field of creating a complex of training specialists. *Trudy uchebnykh zavedenii svyazi = Proceedings of Educational Institutions of Communication*. 2019;(5):78–94. (In Russ.)

14. Lipatnikov V.A., Petrenko M.I. A model of a self-organizing radio communication network functioning in a complex signal-interference environment. *Trudy uchebnykh zavedenii svyazi = Proceedings of Educational Institutions of Communication*. 2023;(9):72–80. (In Russ.)

15. Tomakova R.A., Filist S.A., Brezhnev A.N., et al. The method and algorithm of autonomous flight trajectory planning of an unmanned aerial vehicle when monitoring the fire situation in order to detect the source of ignition early. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2023;13(1):93–110. (In Russ.)

16. Kuleshova E.A., Tanygin M.O. Investigation of the characteristics of modern pseudorandom sequence generators. *Telekommunikatsii = Telecommunications*. 2023;(7):28–39. (In Russ.)

17. Filist S.A., Tomakova R.A., Nefedov N.G., et al. Intelligent image processing system obtained from unmanned aerial vehicles. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2022;12(4):64–85. (In Russ.)

18. Larin S.N., Ermakova I.M. Integrated assessment of innovative software projects quality: a system of indicators. *International Journal of Humanities and Natural Sciences*. 2022;(3-3):179–184.

19. Andronov V.G., Chuev A.A., Knyazev A.A. Model of parameters of deviations of the flight route of unmanned aerial vehicles from a given trajectory. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2021;25(4):145–161. https://doi.org/10.21869/2223-1560-2021-25-4-145-161

20. Mukhin I.E., Tyapkin S.A., Koptev D.S., Shuklina Yu.V. The use of vibration signal structure indicators to solve the problems of diagnosing the technical condition of critical units of modern aircraft. *Telekommunikatsii = Telecommunications*. 2023;(6):2–14. (In Russ.) https://doi.org/10.31044/1684-2588-2023-0-6-2-14. EDN ZCPQKS

Информация об авторах / Information about the Authors

Хмелевская Алена Валентиновна, старший преподаватель кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: aquarel85@mail.ru, ORCID: 0000-0003-0656-1223

Alena V. Khmelevskaya, Senior Lecturer of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: aquarel85@mail.ru, ORCID: 0000-0003-0656-1223

Бабанин Иван Геннадьевич, кандидат технических наук, доцент кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: babanin_ivan@bk.ru, ORCID: 0000-0001-6114-871X

Ivan G. Babanin, Candidate of Sciences (Engineering), Associate Professor of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: babanin_ivan@bk.ru, ORCID: 0000-0001-6114-871X

Севрюков Александр Евгеньевич, доцент кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: alsevryukov@yandex.ru, ORCID: 0009-0002-7234-5983

Alexander E. Sevryukov, Associate Professor of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: alsevryukov@yandex.ru, ORCID: 0009-0002-7234-5983

Николаенко Антон Игоревич, аспирант кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: nikolaenkoai@yandex.ru, ORCID: 0009-0001-7423-0103

Anton I. Nikolaenko, Post-Graduate Student of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: nikolaenkoai@yandex.ru, ORCID:0009-0001-7423-0103

Бабанина Екатерина Юрьевна, магистрант кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: babanina@internet.ru, ORCID: 0009-0001-8014-6506

Севрюков Антон Александрович, специалист по тестированию, ООО «Эдвансед Трансформейшн Консалтинг», г. Москва, Российская Федерация, e-mail: tony.sevryukov@ internet.ru, ORCID: 0009-0009-7027-8124

Ekaterina Yu. Babanina, Undergraduate of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: babanina@internet.ru, ORCID: 0009-0001-8014-6506

Anton A. Sevryukov, Testing Specialist, Advanced Transformation Consulting LLC, Moscow, Russian Federation, e-mail: tony.sevryukov@ internet.ru, ORCID: 0009-0009-7027-8124