ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
http://siit.ugatu.su 2026. Т. 8, № 3(27)
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.056.5:629.7.05 DOI: 10.54708/SIIT-2026-no3-p91 EDN: KSLRUO

Методика интегрированной количественной оценки защищённости навигационной информации беспилотных летательных аппаратов лёгкого класса в условиях деструктивного воздействия

Д. Г. Волошин

Северо-Кавказский федеральный университет

Целью исследования является разработка методики количественной оценки защищённости навигационной информации беспилотных летательных аппаратов (БПЛА) лёгкого класса, дающую единый численный показатель и учитывающую ресурсные и эксплуатационные ограничения платформы. Методика опирается на вероятностно-рисковый подход: для каждой пары «угроза – уязвимость» вычисляется риск эксплуатации с учётом вероятности обнаружения угрозы, условной вероятности успешной эксплуатации, эффективности наиболее сильной применимой меры защиты и коэффициента критичности подсистемы; частные риски агрегируются во взвешенный интегральный показатель защищённости, корректируемый адаптивными коэффициентами электромагнитной обстановки, географии и интенсивности атак. Достоверность подтверждена сопоставлением с методикой NIST SP 800-30 и экспертной валидацией. На примере квадрокоптера лёгкого класса массой до 25 кг интегральный показатель защищённости при базовой конфигурации составил 0,329 (низкий уровень) и возрос до 0,894 (высокий уровень) при полном наборе из шести мер защиты. Наибольший вклад в суммарный риск (около 59,6 %) вносит скрытый GPS-спуфинг. Для бюджетного ограничения 40 тыс. руб. найдено оптимальное подмножество мер, обеспечивающее показатель 0,822 при стоимости 35 тыс. руб. Учёт реальных условий эксплуатации снижает эффективную защищённость до 0,48-0,53. Предложенная методика обеспечивает сопоставимую количественную оценку альтернативных конфигураций защиты лёгких БПЛА и применима на этапах проектирования, модернизации и планирования миссии. Практическая значимость состоит в возможности обоснованного выбора набора мер защиты в условиях ограничений по стоимости и энергопотреблению.

Беспилотный летательный аппарат; оценка защищённости; интегральный показатель; вероятностный подход; GPS-спуфинг; риск эксплуатации уязвимостей; адаптивные коэффициенты среды; оптимизация мер защиты.

Введение

За последние годы область применения беспилотных летательных аппаратов (БПЛА) лёгкого класса заметно расширилась – от мониторинга сельскохозяйственных угодий и аэрофотосъёмки до доставки малогабаритных грузов до решения разведывательных задач [Гур24, Саи25]. Параллельно с ростом парка увеличивается и число угроз бортовым системам: радиоэлектронное подавление, кибератаки на каналы управления и навигации, физическое воздействие на аппарат. Особую опасность представляют спуфинг-атаки на навигационные сигналы, при которых подлинный сигнал глобальной навигационной спутниковой системы (ГНСС) незаметно подменяется, и аппарат, продолжая полёт, следует по ложной траектории.

Практическая потребность здесь сводится к тому, что разработчику и эксплуатанту нужен инструмент, позволяющий не просто перечислять угрозы, а численно оценивать, насколько

Волошин Д. Г. Методика интегральной количественной оценки защищённости навигационной информации беспилотных летательных аппаратов лёгкого класса в условиях деструктивного воздействия // СИИТ. 2026. Т. 8, № 3(27). С. 91-104. DOI: 10.54708/SIIT-2026-no3-p91. EDN: KSLRUO.

Voloshin D. G. Methodology for the integrated quantitative assessment of the security of navigation information of light unmanned aerial vehicles under destructive impact conditions // SIIT. 2026. Vol. 8, no. 3(27), pp. 91-104. DOI: 10.54708/SIIT-2026-no3-p91. EDN: KSLRUO. (In Russian).

конкретная конфигурация БПЛА способна им противостоять, и сопоставлять по этому показателю альтернативные архитектурные решения. Значительная часть предложенных к настоящему времени методов использует качественные шкалы вида «низкий–средний–высокий», которые не дают формально сравнить два варианта защиты. Работы с количественными метриками, как правило, ограничены одной категорией угроз – либо киберугрозами, либо радиоэлектронным противодействием, либо физическим воздействием – и не сводят результат в единый показатель. Между тем именно интегральный индекс позволяет на этапе проектирования, модернизации или планирования миссии сравнивать варианты в численном виде. В отечественной нормативной повестке запрос на подобный инструментарий зафиксирован, в частности, в Стратегии развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года.

Дополнительное осложнение связано с самим классом аппаратов. Масса, габариты, энергопотребление и стоимость лёгких БПЛА не позволяют устанавливать ресурсоёмкие защитные решения, применяемые в пилотируемой или военной авиации, поэтому оценка защищённости должна явно учитывать ресурсные ограничения платформы. Существующие универсальные методики управления рисками этого ограничения не отражают.

Целью настоящей работы является разработка методики количественной оценки защищённости навигационной информации БПЛА лёгкого класса, дающей единый численный показатель и учитывающей ресурсные и эксплуатационные ограничения платформы. Для достижения цели решаются следующие задачи: формализация множеств угроз, уязвимостей и мер защиты применительно к лёгкому БПЛА; построение вероятностной модели риска пары «угроза–уязвимость» с учётом критичности поражаемой подсистемы; формализация правил агрегирования и адаптации интегрального показателя к условиям эксплуатации; разработка процедуры экспертного оценивания параметров с контролем согласованности; проверка методики на тестовом примере и сопоставление с эталонными методиками управления рисками.

Постановка задачи и анализ известных подходов

Защищённость БПЛА при внешних воздействиях рассматривается в ряде отечественных и зарубежных исследований. В отечественной литературе значительное внимание уделено радиоэлектронному противодействию: в работах С. И. Макаренко [Мак20а, Мак20б] выполнен системный анализ средств радиоэлектронной борьбы с беспилотными аппаратами, рассмотрены методы подавления каналов связи и навигации, классифицированы существующие комплексы. Эти исследования формируют теоретическую базу анализа радиоэлектронных угроз, однако ориентированы преимущественно на задачи противодействия БПЛА, а не на оценку защищённости самих аппаратов. Вопросы обнаружения кибератак на борту отражены, в частности, в проекте РНФ № 21-79-00194 [Бас21], где предложена система самодиагностики на основе анализа изменения параметров бортовых подсистем; такой подход выявляет аномалии в работе аппарата, но не формирует интегрального показателя защищённости.

Методологическую основу количественной оценки формируют исследования по безопасности автоматизированных и распределённых систем. В [Тра24] предложена марковская модель кибератак для анализа защищённости в автоматизированных системах управления; в [Бар24] сформулированы частные показатели эффективности защищённости объектов информационной инфраструктуры; в [Кор23] представлен вероятностный подход к комплексной оценке защищённости информации в системах критического назначения; в [Скр24а, Скр24b] рассмотрены процедуры количественной оценки и управляемости защищённостью. Общим ограничением этих методов является их стационарность: они создавались под корпоративные и распределённые системы и не учитывают характерные для БПЛА подвижность, жёсткий дефицит энергоресурса и высокую зависимость от радиоканала и сигналов ГНСС [Fri17, Хал25, Пет26].

В зарубежной литературе акценты смещены на специализированные угрозы, прежде всего на GPS-спуфинг. Обзорные работы по кибератакам на авионику БПЛА и применимым контрмерам приведены в [Yu24, Tsa22, Kum24]. Методы обнаружения спуфинга развиваются в нескольких направлениях: в [Wei22] предложен подход на основе семантики управления и одномерных свёрточных сетей для применения в реальном времени, в [Ma25] – ансамблевый метод с использованием свёрточных сетей и алгоритма градиентного бустинга. Эти методы эффективны для отдельных классов атак, но не решают задачу комплексной оценки защищённости. Универсальные методологии управления рисками представлены в NIST SP 800-30 [NIS12], ISO/IEC 27005 [ISO22] и каталогом тактик и техник MITRE ATT&CK [MIT26]; они широко применяются, но изначально формировались под корпоративные информационные системы и единой интегральной метрики, учитывающей киберфизическую специфику БПЛА, не задают.

Проведённый анализ показывает, что метод, дающий комплексную количественную оценку защищённости сразу по трём группам угроз – радиоэлектронным, кибернетическим и физическим – и при этом учитывающий ресурсные и эксплуатационные ограничения лёгкого аппарата, до настоящего времени не предложен. Это и определяет постановку задачи: построить интегральную количественную оценку защищённости БПЛА (ИКОЗ-БПЛА).

Предлагаемая методика количественной оценки защищённости навигационной информации БПЛА лёгкого класса в условиях деструктивного воздействия

Методика строится на вероятностно-рисковом подходе, исходящем из того, что абсолютная защита недостижима и корректнее говорить о снижении риска до приемлемого уровня. В отличие от качественных шкал, методика оперирует количественными метриками, что позволяет сравнивать конфигурации, оптимизировать состав средств защиты и прогнозировать поведение системы при деструктивных воздействиях. Процедура оценки включает пять последовательных этапов. Их общая последовательность и взаимосвязь показаны на рис. 1.

Рис. 1 Схема методики ИКОЗ-БПЛА

Как видно, методика организована в виде сквозной цепочки этапов: результаты идентификации и вероятностной оценки последовательно преобразуются в матрицу рисков, затем сворачиваются в единый показатель и, наконец, корректируются под условия применения. Такая структура обеспечивает прослеживаемость расчёта от исходных данных до итоговой оценки. Ниже приведено описание этапов 1–5 методики.

Этап 1. Идентификация и классификация компонентов. Формируется множество угроз $U = \{u_1, \dots, u_m\}$, разделённых на три категории – радиоэлектронные (подавление навигационных сигналов и каналов связи, открытый, скрытый и ретрансляционный спуфинг), кибернетические (атаки «человек посередине» на канал управления, внедрение вредоносного кода, отказ в обслуживании, перехват телеметрии) и физические (кинетическое поражение, лазерное и акустическое воздействие на датчики). Каждой угрозе u_i присваивается весовой коэффициент $w_i \in [0,1]$, отражающий её критичность для типовой миссии, при условии нормировки

$$\sum_{i=1}^{m} w_i = 1. \quad (1)$$

Далее формируется множество уязвимостей $V = \{v_1, \dots, v_n\}$, каждой из которых ставится в соответствие коэффициент критичности $C(v_j)$, характеризующий важность поражаемой подсистемы:

$$C(v_j) = \begin{cases} 1{,}0, & \text{критические системы (навигация, управление)}, \\ 0{,}7, & \text{важные (связь, ПО)}, \\ 0{,}4, & \text{вспомогательные}. \end{cases} \quad (2)$$

Замыкает этап описание множества мер защиты $D = \{d_1, \dots, d_k\}$ – технических (криптографические модули, экранирование) и алгоритмических (детекция аномалий, процедуры автономной навигации), соотнесённых с уязвимостями, которые они призваны нейтрализовать.

Этап 2. Определение вероятностных параметров. Для каждой угрозы определяется вероятность её обнаружения $P_{\text{обн}}(u_i)$, зависящая от эффективности бортовых средств мониторинга (0,9-0,95 при наличии специализированных алгоритмов детекции; 0,5–0,7 при косвенных методах; 0,1–0,3 при их отсутствии). Для каждой релевантной пары «угроза–уязвимость» оценивается условная вероятность успешной эксплуатации $P_{\text{уязв}}(u_i, v_j)$, зависящая от сложности атаки, доступности инструментария и квалификации нарушителя. Эффективность меры d_l против уязвимости v_jобозначается $E(d_l, v_j) \in [0,1]$ и раскладывается на три сомножителя:

$$E(d_l, v_j) = E_{\text{тех}}(d_l, v_j) E_{\text{реал}}(d_l) E_{\text{акт}}(d_l), \quad (3)$$

где $E_{\text{тех}}$ отражает технический потенциал меры, $E_{\text{реал}}$ – качество её реализации, $E_{\text{акт}}$ – актуальность с учётом появления новых методов атак.

Этап 3. Расчёт риска эксплуатации уязвимостей. Риск для пары «угроза–уязвимость» вычисляется как

$$R(u_i, v_j) = P_{\text{обн}}(u_i) P_{\text{уязв}}(u_i, v_j) \left(1 - \max_{d \in D} E(d, v_j)\right) C(v_j), \quad (4)$$

где множитель $\left(1 - \max_{d \in D} E(d, v_j)\right)$ задаёт долю остаточного риска и отражает ориентир на наиболее сильную из применимых к данной уязвимости мер защиты. Все вычисленные значения $R(u_i, v_j)$сводятся в матрицу рисков, анализ которой выявляет наиболее критичные сочетания угроз и уязвимостей. Структура самой модели риска для одной пары «угроза – уязвимость» показана на рис. 2, а полученная для рассматриваемого аппарата матрица остаточных рисков – на рис. 3. Рис. 2 поясняет смысл формулы (4): итоговый риск пары образуется произведением четырёх сомножителей – вероятности обнаружения угрозы, условной вероятности эксплуатации, доли остаточного риска после применения сильнейшей меры и коэффициента критичности поражаемой подсистемы. Обнуление любого из них резко снижает вклад пары в суммарный риск.

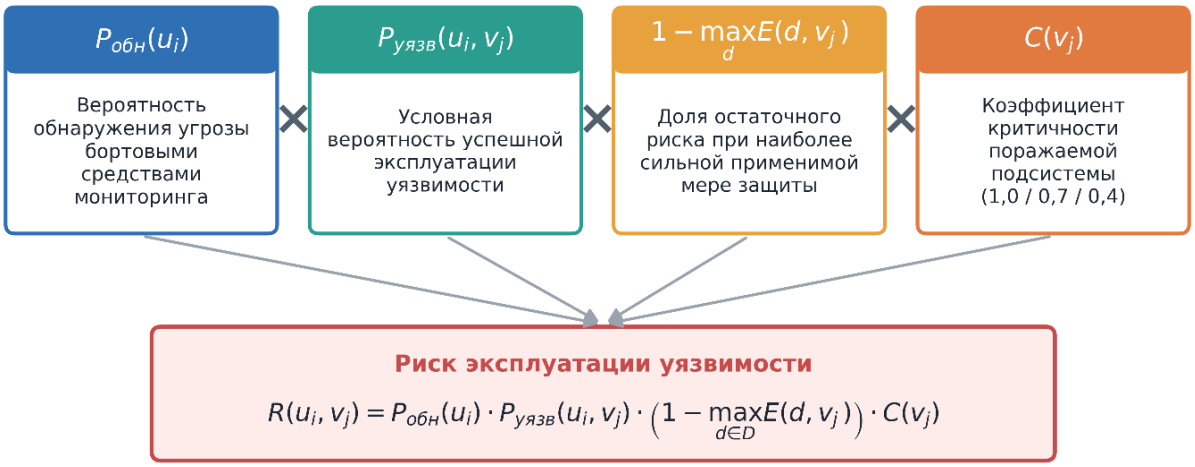

Рис. 2 Структура модели риска пары «угроза – уязвимость»

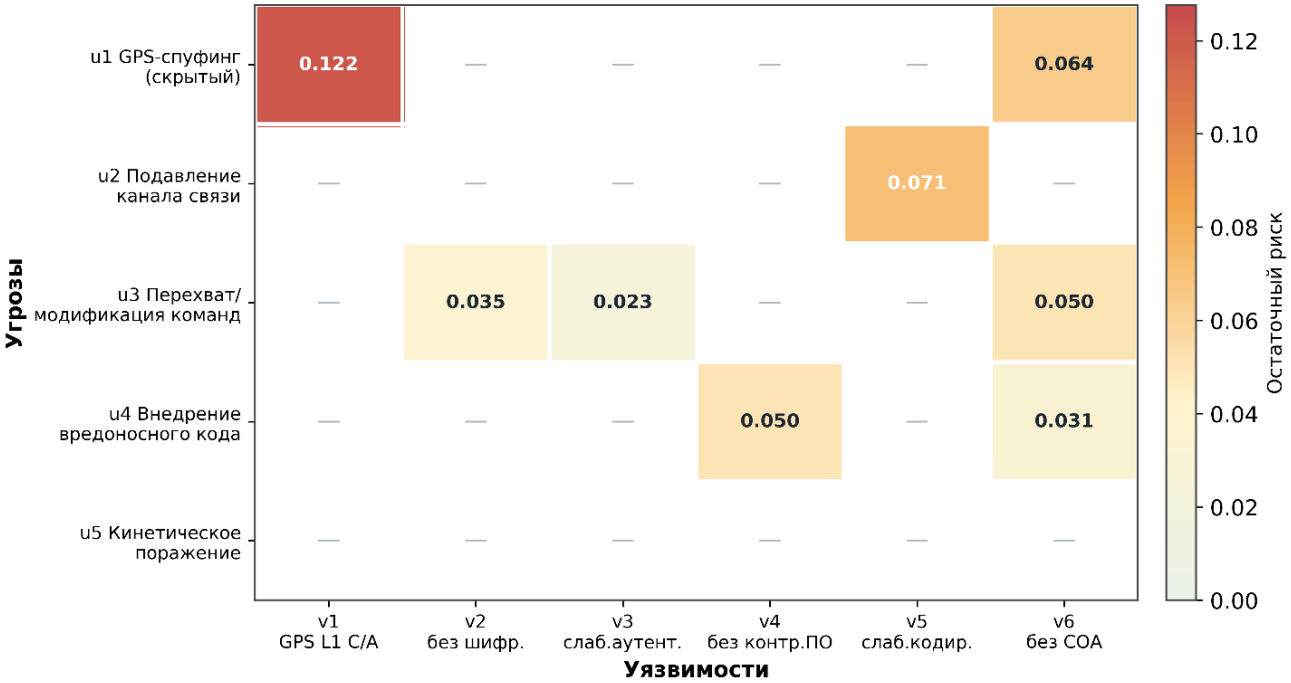

Рис. 3 Матрица остаточных рисков $P(u_i, v_j)$ при наличии мер защиты: цвет ячейки отражает величину остаточного риска $R(u_i, v_j)$; красным квадратом выделена доминирующая пара «скрытый GPS-спуфинг – незащищённый сигнал GPS L1 C/A» со значением 0,122, дающая наибольший вклад в суммарный риск

Из рис. 3 видно, что наибольший остаточный риск сосредоточен в верхней левой ячейке – на паре скрытого GPS-спуфинга и незащищённого сигнала GPS L1 C/A; остальные сочетания дают заметно меньший вклад, что задаёт приоритет при выборе мер защиты.

Этап 4. Агрегирование и расчёт интегральной защищённости. Интегральный показатель защищённости вычисляется как дополнение взвешенного суммарного риска до единицы:

$$Z_{\text{БПЛА}} = 1 - \sum_{i=1}^{m} \sum_{j=1}^{n} w_i \, R(u_i, v_j), \tag{5}$$

где m – число типов угроз, n – число уязвимостей. Значению $Z_{\text{БПЛА}} = 1$ соответствует нулевой остаточный риск, значению 0 – полная уязвимость; любое увеличение суммарного риска ведёт к монотонному убыванию показателя.

Этап 5. Адаптация к условиям функционирования. Для перехода от интегральной оценки к реалистичной интегральный показатель корректируется набором адаптивных коэффициентов $\beta_k \in (0,1]$:

$$Z_{\text{адапт}} = Z_{\text{БПЛА}} \prod_{k=1}^{p} \beta_k \,(\text{условия}_k). \quad (6)$$

В работе используются три коэффициента:

1) коэффициент электромагнитной обстановки $\beta_{\text{ЭМО}}$, который задаётся дискретной зависимостью от отношения сигнал/шум SNR: 1,0 при SNR > 20 дБ; 0,9 при 15–20 дБ; 0,7 при 10–25 дБ; 0,5 при 5–10 дБ; 0,3 при SNR < 5 дБ.

2) коэффициент интенсивности атак $\beta_{\text{угроз}} = \max(0{,}3;\ 1 - k \cdot \ln(1 + I_{\text{атак}}))$, где $I_{\text{атак}}$ – наблюдаемая интенсивность атак (попыток в час), $k \approx 0{,}045$ – калибровочный коэффициент, при котором для типового диапазона 1-10 попыток в час значение $\beta_{\text{угроз}}$ остаётся в коридоре 0,9-0,97.

3) коэффициент географических условий $\beta_{\text{гео}}$ принимает значения 1,0 для открытой местности, 0,85 для полугородской застройки и 0,7 для плотной городской застройки.

Процедура определения параметров методом экспертных оценок

Вероятностные параметры методики определяются структурированным экспертным опросом. Экспертная группа формируется с охватом профилей информационной безопасности БПЛА, радиоэлектронных систем и навигации, разработки бортового программного обеспечения и испытаний; каждый эксперт должен иметь опыт работы по профилю не менее пяти лет и подтверждённую квалификацию. Согласованность мнений контролируется коэффициентом конкордации Кендалла

$$W = \frac{12S}{K^2(N^3 - N)}, \quad (7)$$

где S – сумма квадратов отклонений суммарных рангов от среднего, K – число экспертов, N – число оцениваемых объектов. Значимость W проверяется по критерию χ^2 с $N - 1$ степенями свободы; приемлемой считается согласованность при $W \geq 0{,}7$. Итоговые значения параметров получаются как взвешенное среднее оценок экспертов с весами, вычисляемыми из композита компетентности (образование, опыт, научная активность) с последующей нормировкой к единице. При недостаточной согласованности проводится повторный тур по процедуре Делфи.

Результаты вычислительного эксперимента

Практическая применимость методики проверена на примере типового квадрокоптера лёгкого класса массой до 25 кг, используемого для мониторинга и разведки. Рассматривается сценарий ведения разведки в полугородской местности с высоким уровнем электромагнитных помех и средним уровнем киберугроз.

Исходные данные получены структурированным опросом группы из пяти экспертов; коэффициент конкордации Кендалла составил $W = 0{,}74$ при $\chi^2_{\text{расч}} = 11{,}1$ (число объектов $N = 4$, число экспертов $K = 5$), что превышает критическое значение $\chi^2_{0{,}05;3} = 7{,}815$; согласованность статистически значима на уровне $\alpha = 0{,}05$, повторные туры не потребовались. Перечень рассматриваемых угроз с их весовыми коэффициентами и вероятностями обнаружения приведён в табл. 1.

Весовые коэффициенты отражают относительную значимость каждой угрозы для лёгкого БПЛА в заданном сценарии. Кинетическое поражение (u_5) включено в перечень как внешняя физическая угроза, однако в рамках информационной защищённости оно не эксплуатирует

программно-аппаратных уязвимостей навигационного контура, что отражается далее в матрице вероятностей эксплуатации. Учитываемые уязвимости и присвоенные им коэффициенты критичности сведены в табл. 2.

Таблица 1

Угрозы u_i, их весовые коэффициенты w_i и вероятности обнаружения $P_{\text{обн}}(u_i)$

№	Угроза u_i	Вес w_i	$P_{\text{обн}}(u_i)$
u_1	GPS-спуфинг (скрытый)	0,30	0,65
u_2	Подавление канала связи	0,25	0,90
u_3	Перехват и модификация команд	0,20	0,55
u_4	Внедрение вредоносного кода	0,15	0,30
u_5	Кинетическое поражение	0,10	0,95

Таблица 2

Уязвимости v_j и их критичность $C(v_j)$

№	Уязвимость v_j	Критичность $C(v_j)$
v_1	Использование только GPS L1 C/A	1,0 (навигация)
v_2	Отсутствие шифрования канала связи	1,0 (управление)
v_3	Слабая аутентификация команд	1,0 (управление)
v_4	Отсутствие контроля целостности ПО	0,7 (ПО)
v_5	Недостаточное помехоустойчивое кодирование	0,7 (связь)
v_6	Отсутствие системы обнаружения аномалий	0,7 (ПО)

Условные вероятности успешной эксплуатации каждой уязвимости соответствующей угрозой представлены в табл. 3.

Таблица 3

Матрица вероятностей эксплуатации уязвимостей $P_{\text{уязв}}(u_i, v_j)$

Угроза / уязвимость	v_1	v_2	v_3	v_4	v_5	v_6
u_1	0,85	–	–	–	–	0,70
u_2	–	–	–	–	0,75	–
u_3	–	0,90	0,85	–	–	0,65
u_4	–	–	–	0,80	–	0,75
u_5	–	–	–	–	–	–

Прочерк означает, что соответствующая угроза напрямую не эксплуатирует данную уязвимость. Так, скрытый GPS-спуфинг (u_1) с высокой вероятностью (0,85) эксплуатирует использование незащищённого гражданского сигнала GPS L1 C/A (v_1); кинетическое поражение (v_5) не эксплуатирует ни одной из информационных уязвимостей навигационного контура. Эффективность рассматриваемых мер защиты по отношению к каждой уязвимости задана в табл. 4. Наибольшую эффективность обеспечивают криптографические меры (шифрование канала и цифровая подпись команд), тогда как алгоритмические средства детекции дают более умеренный, но устойчивый вклад. Расчёт базовой конфигурации (меры защиты отсутствуют, $\max_d E = 0$) сводит частный риск к произведению $P_{\text{обн}} P_{\text{уязв}} C$. Суммарный взвешенный риск при этом составляет 0,671, откуда интегральный показатель защищённости базовой конфигурации

$$Z_0 = 1 - 0{,}671 = 0{,}329, \tag{8}$$

что соответствует низкому уровню и указывает на высокую уязвимость типовых коммерческих и полупрофессиональных аппаратов перед радиоэлектронными и кибернетическими угрозами. Наибольший индивидуальный риск приходится на пару «скрытый GPS-спуфинг – незащищённый сигнал GPS L1 C/A» ($R \approx 0{,}1216$ при наличии меры детекции), а суммарно угроза GPS-спуфинга формирует около 59,6% взвешенного риска.

Таблица 4

Матрица эффективности мер защиты $E(d_l, v_j)$

Мера / уязвимость	v_1	v_2	v_3	v_4	v_5	v_6
d_1 – интеграция GPS/INS (фильтр Калмана)	0,65	–	–	–	–	–
d_2 – детекция спуфинга по фазе несущей	0,78	–	–	–	–	–
d_3 – шифрование канала AES-256-GCM	–	0,93	–	–	–	–
d_4 – цифровая подпись команд (ГОСТ Р 34.10-2012)	–	–	0,95	–	–	–
d_5 – помехоустойчивое кодирование LDPC	–	–	–	–	0,85	–
d_6 – система обнаружения вторжений (ML)	–	–	–	0,70	–	0,80

Введение полного набора из шести мер защиты повышает интегральный показатель до

$$Z = 1 - 0{,}107 = 0{,}894, \tag{9}$$

т. е. до высокого уровня. Прирост относительно базовой конфигурации составляет 0,565. Анализ чувствительности показывает, что варьирование эффективности ключевой меры детекции спуфинга $E(d_2, v_1)$ в диапазоне 0,6-0,9 изменяет итоговую защищённость на 4,4% (нелинейная зависимость), а перераспределение весов в пользу киберугроз смещает оценку не более чем на 2,3%, что свидетельствует об устойчивости результата и сбалансированности набора мер. Сравнение базовой и защищённых конфигураций по интегральному показателю приведено на рис. 4.

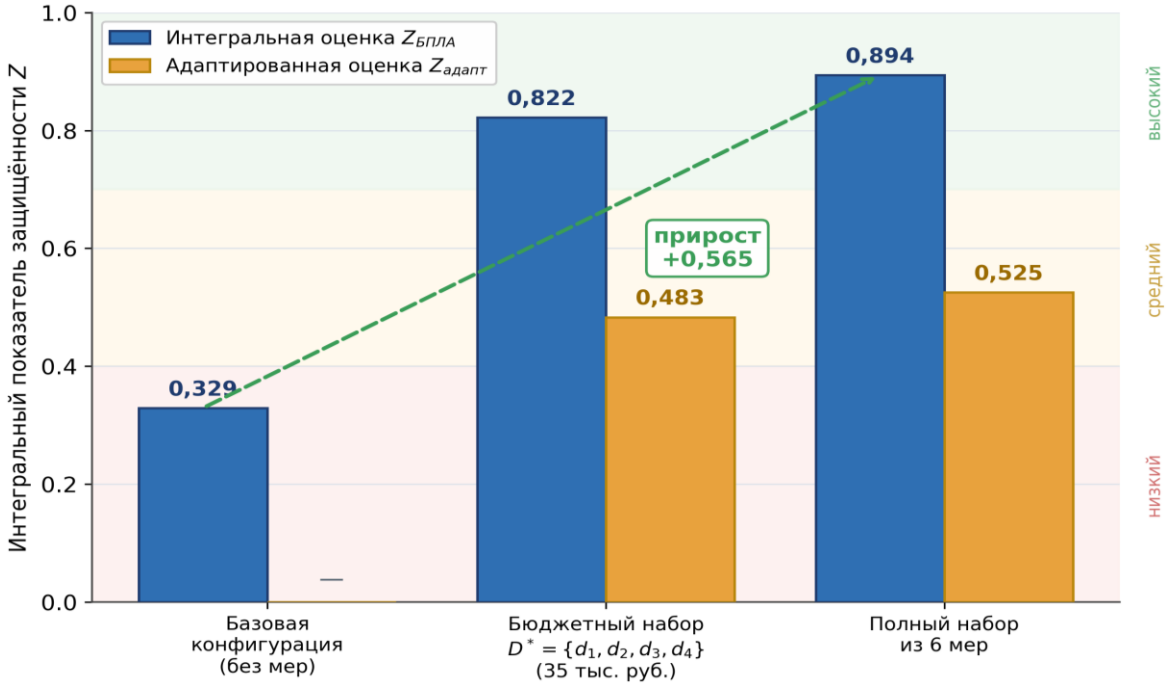

Рис. 4 Сравнение конфигураций защиты лёгкого БПЛА:
синие столбцы – интегральная оценка $Z_{БПЛА}$ для базовой, бюджетной и полной конфигураций; оранжевые – адаптированная оценка $Z_{адапт}$ с учётом условий эксплуатации; прирост +0,565 показывает рост защищённости при переходе от базовой конфигурации к полному набору мер

Рис. 4 наглядно показывает разрыв между конфигурациями: базовый вариант остаётся в зоне низкой защищённости, тогда как полный и бюджетный наборы мер переводят аппарат в область высоких значений, причём адаптированные оценки во всех случаях заметно ниже интегральных. Для сценария полугородской застройки при SNR ≈ 12 дБ (что даёт $\beta_{\text{ЭМО}} = 0{,}70$), эффекте многолучевого распространения ($\beta_{\text{гео}} = 0{,}85$) и средней интенсивности атак $I_{\text{атак}} \approx 4{,}7$ попыток в час ($\beta_{\text{угроз}} = 0{,}92$) адаптивная защищённость полного набора мер составляет $Z_{\text{адапт}} \approx 0{,}525$. Снижение относительно интегральной оценки на величину порядка 37% количественно подтверждает необходимость включения параметров внешней среды в расчётную модель и показывает ограниченность «лабораторных» оценок безопасности. Последовательное влияние каждого из адаптивных коэффициентов на итоговую оценку иллюстрирует рис. 5.

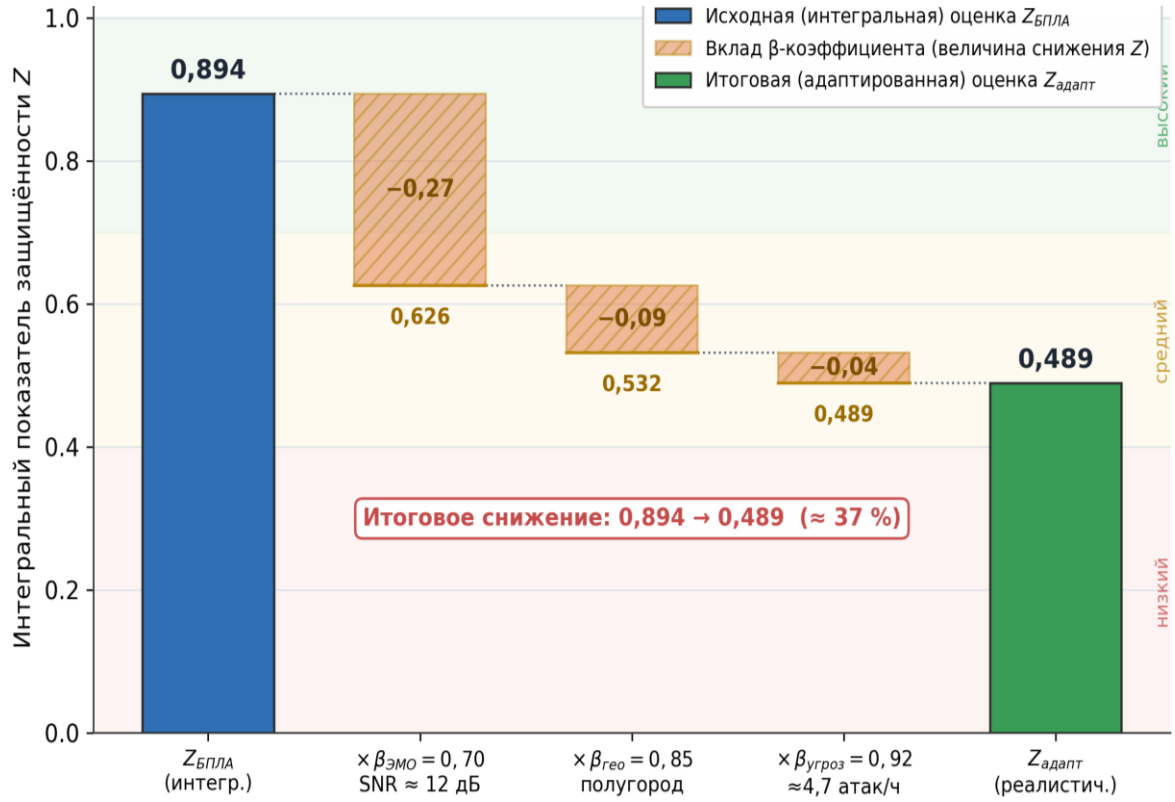

Рис. 5 Влияние адаптивных коэффициентов среды на защищённость для полного набора из шести мер в сценарии полугородской застройки: исходная интегральная оценка $Z_{\text{БПЛА}}$ последовательно снижается коэффициентами $\beta_{\text{ЭМО}}$, $\beta_{\text{гео}}$ и $\beta_{\text{угроз}}$ до адаптированной оценки $Z_{\text{адапт}}$; штриховые столбцы показывают вклад каждого коэффициента в снижение

Как показано на рис. 5, основной вклад в снижение даёт коэффициент электромагнитной обстановки, а география и интенсивность атак уменьшают показатель дополнительно; суммарно это и формирует переход из зоны высокой защищённости в зону средней. Задача выбора оптимального подмножества мер $D^* \subseteq D$ решается при ограничениях на суммарную стоимость $C_{\max} = 40\,000$ руб. и прирост энергопотребления $\Delta E_{\max} = 10\,\%$ как задача о ранце с целевой функцией максимизации $Z_{\text{БПЛА}}$.

Удельная эффективность мер (прирост защищённости на единицу стоимости $\Delta Z/C$) приведена в табл. 5.

Таблица 5

Прирост защищённости на единицу стоимости для мер защиты

Мера	Стоимость, руб.	Прирост ΔZ	Эффективность $\Delta Z/C$
d_3	5 000	0,215	0,0430
d_4	7 000	0,178	0,0254
d_2	8 000	0,189	0,0236
d_1	15 000	0,153	0,0102
d_5	10 000	0,098	0,0098
d_6	20 000	0,134	0,0067

Из табл. 5 следует, что удельная эффективность мер различается более чем на порядок: дешёвые криптографические меры дают наибольший прирост защищённости на рубль, тогда как ресурсоёмкая система обнаружения вторжений – наименьший. Те же данные в графическом виде, упорядоченные по убыванию удельной эффективности, представлены на рис. 6.

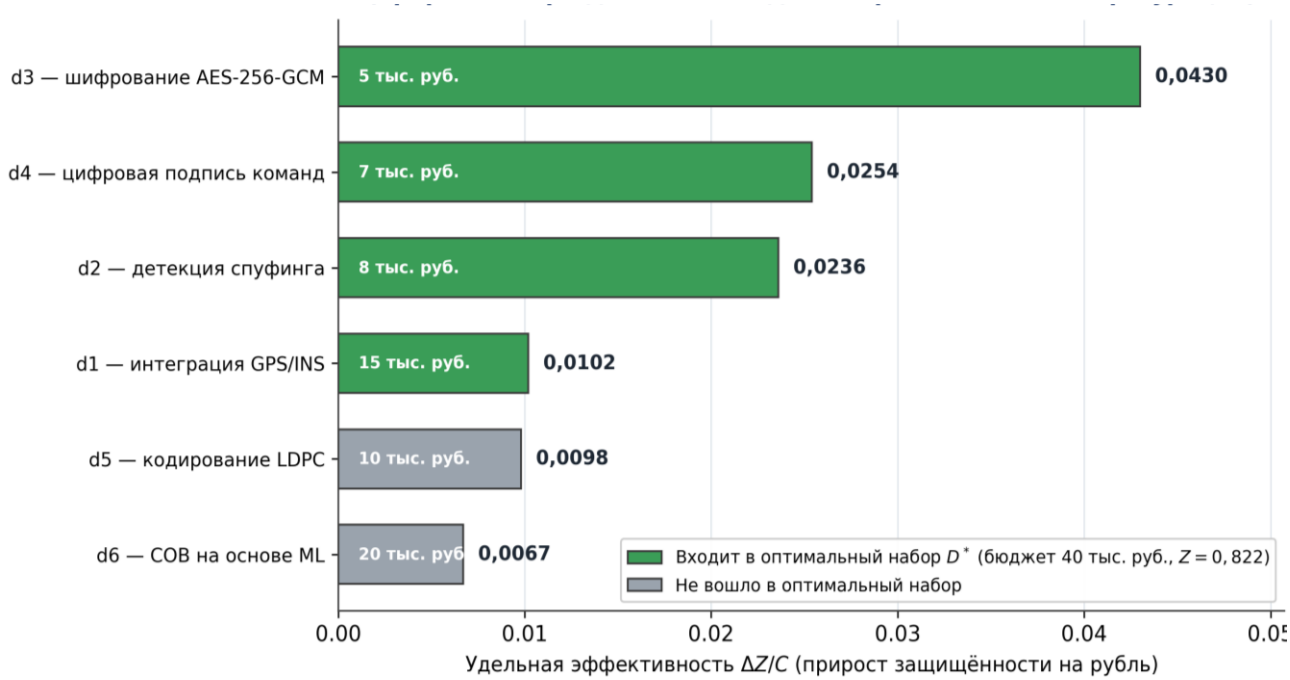

Рис. 6 Ранжирование мер защиты по удельной эффективности: приведён прирост защищённости на единицу стоимости ΔZ/C при добавлении одной меры к базовой конфигурации; зелёным выделены меры, входящие в оптимальный по бюджету набор *D**, серым – не вошедшие в него

Рис. 6 подтверждает порядок предпочтения мер, где в оптимальное по бюджету подмножество входят четыре наиболее эффективные меры, тогда как замыкающие ранжирование средства оправданы лишь при наличии свободного ресурса. Ранжирование по удельной эффективности даёт порядок $d_3 \to d_4 \to d_2 \to d_1 \to d_5 \to d_6$. При бюджете 40 000 руб. оптимальным является набор $D^* = \{d_1, d_2, d_3, d_4\}$ суммарной стоимостью 35 000 руб. и приростом энергопотребления +8 %, обеспечивающий защищённость $Z = 0{,}822$ (около 92% от максимально достижимой при 78% полной стоимости) и адаптивную защищённость $Z_{\text{адапт}} = 0{,}483$. Наибольшую удельную эффективность дают криптографическая защита канала и алгоритм обнаружения GPS-спуфинга; система обнаружения вторжений на основе машинного обучения в ресурсных ограничениях лёгкого БПЛА показывает наименьшую удельную эффективность и оправдана лишь при наличии свободного вычислительного ресурса.

Обсуждение

Для проверки достоверности результаты сопоставлены с оценкой по методике NIST SP 800-30 на качественной шкале. Базовая конфигурация по обоим подходам относится к категории «низкий – средний» уровень защищённости, конфигурация с полным набором мер – к категории «высокий», то есть упорядоченность конфигураций сохраняется. При этом предлагаемая методика даёт непрерывную числовую оценку и за счёт адаптивных коэффициентов среды различает конфигурации в пределах одной качественной категории риска, чего качественные шкалы не позволяют. Результаты вынесены на оценку экспертной группы: четверо из пяти экспертов сочли их соответствующими реальной обстановке, один предложил скорректировать веса угроз; после корректировки итоговое значение сместилось на 2,3 %, что подтверждает устойчивость метода.

В отличие от ISO/IEC 27005 и MITRE ATT&CK, ориентированных на корпоративные информационные системы, методика ИКОЗ-БПЛА формирует единый интегральный показатель, адаптированный к киберфизической природе аппарата, и формализует влияние внешней среды через корректирующие коэффициенты, что делает её пригодной для планирования миссий и оперативной оценки рисков. К ограничениям метода относятся зависимость от экспертных оценок и ориентация преимущественно на лёгкий класс, что требует дополнительной калибровки для других типов аппаратов. Дальнейшее развитие связано с формированием типовой базы угроз и мер защиты, интеграцией статистики инцидентов, учётом временной динамики старения защитных мер и автоматизацией обновления параметров.

Заключение

Разработана методика интегральной количественной оценки защищённости навигационной информации лёгких БПЛА (ИКОЗ-БПЛА), возвращающая единый численный показатель $Z \in [0, 1]$ и в отличие от качественных и узкоспециализированных подходов учитывающая три группы угроз, критичность поражаемых подсистем и ресурсные ограничения платформы. На примере квадрокоптера лёгкого класса показано, что внедрение полного набора из шести мер повышает показатель защищённости с 0,329 до 0,894, а оптимальное по бюджету подмножество из четырёх мер обеспечивает 0,822 при стоимости 35 тыс. руб. Учёт реальных условий эксплуатации снижает эффективную защищённость до 0,48-0,53, что количественно обосновывает включение адаптивных коэффициентов среды в расчётную модель. Сопоставление с NIST SP 800-30, ISO/IEC 27005 и MITRE ATT&CK подтвердило концептуальную согласованность методики при более высокой количественной детализации. Методика применима для оценки текущего уровня защищённости и для поддержки решений при выборе набора мер защиты в условиях ограничений по стоимости и энергопотреблению на этапах проектирования, модернизации и эксплуатации БПЛА лёгкого класса.

Перспективные направления дальнейших исследований связаны прежде всего с преодолением выявленных ограничений методики ИКОЗ-БПЛА – зависимости от экспертных оценок и ориентации преимущественно на лёгкий класс аппаратов. В их числе: формирование типовой базы угроз, уязвимостей и мер защиты, снижающей субъективность исходных параметров и упрощающей применение методики; интеграция статистики реальных инцидентов и результатов натурных испытаний для калибровки вероятностей обнаружения и успешной эксплуатации угроз; учёт временно́й динамики, отражающей старение мер защиты и появление новых способов атак, в том числе совершенствующихся методов скрытого GPS-спуфинга; автоматизация процедуры расчёта и обновления параметров, а также адаптация модели к другим классам и типам беспилотных аппаратов. Отдельным направлением является экспериментальная верификация интегрального показателя на реальной платформе БПЛА лёгкого класса в условиях деструктивного воздействия для подтверждения соответствия расчётных оценок фактическому уровню защищённости навигационной информации.

СПИСОК ЛИТЕРАТУРЫ | REFERENCES

[Fri17] Frid A. I., Vulfin A. M., et al. Architecture of the security access system for information on the state of automatic control systems of aircraft // CSIT'2017: Proc.19th Int. Workshop, Baden-Baden, Germany. Vol. 1. 2017. P. 16-19. EDN YMGQPR.

Frid A. I., Vulfin A. M., et al. Architecture of the security access system for information on the state of automatic control systems of aircraft // CSIT'2017: Proc.19th Int. Workshop, Baden-Baden, Germany. Vol. 1. 2017. P. 16-19. EDN YMGQPR.

[ISO22] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. International Organization for Standardization, 2022.

ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. International Organization for Standardization, 2022.

[Kum24] Kumar N., Chaudhary A. Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security // Computer Networks. 2024. Vol. 252. Art. 110695. EDN ERTLIC.

Kumar N., Chaudhary A. Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security // Computer Networks. 2024. Vol. 252. Art. 110695. EDN ERTLIC.

[Ma25] Ma T., Zhang X., Miao Z. Detection of UAV GPS spoofing attacks using a stacked ensemble method // Drones. 2025. Vol. 9, № 1. Art. 2. EDN KTIPPI.

Ma T., Zhang X., Miao Z. Detection of UAV GPS spoofing attacks using a stacked ensemble method // Drones. 2025. Vol. 9, № 1. Art. 2. EDN KTIPPI.

[MIT26] MITRE ATT&CK [Электронный ресурс]. URL: https://attack.mitre.org (дата обращения: 20.04.2026)

MITRE ATT&CK [Electronic resource]. URL: https://attack.mitre.org (accessed: April 20, 2026)

[NIS12] NIST Special Publication 800-30 Rev. 1. Guide for conducting risk assessments. National Institute of Standards and Technology, 2012. DOI 10.6028/NIST.SP.800-30r1.

NIST Special Publication 800-30 Rev. 1. Guide for conducting risk assessments. National Institute of Standards and Technology, 2012. DOI 10.6028/NIST.SP.800-30r1.

[Tsa22] Tsao K.-Y., Girdler T., Vassilakis V. G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks // Ad Hoc Networks. 2022. Vol. 133. Art. 102894. EDN DKUBYC.

Tsao K.-Y., Girdler T., Vassilakis V. G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks // Ad Hoc Networks. 2022. Vol. 133. Art. 102894. EDN DKUBYC.

[Wei22] Wei X., Sun C., et al. ConstDet: control semantics-based detection for GPS spoofing attacks on UAVs // Remote Sensing. 2022. Vol. 14, № 21. Art. 5587. EDN XGMFUU.

Wei X., Sun C., et al. ConstDet: control semantics-based detection for GPS spoofing attacks on UAVs // Remote Sensing. 2022. Vol. 14, № 21. Art. 5587. EDN XGMFUU.

[Yu24] Yu A., Kolotylo I., et al. Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics: a survey // arXiv preprint arXiv: 2504.07358. 2024. EDN AKHJLL.

Yu A., Kolotylo I., et al. Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics: a survey // arXiv preprint arXiv: 2504.07358. 2024. EDN AKHJLL.

[Бар24] Барановский О. К. Частные показатели эффективности защищённости объектов информационной инфраструктуры от кибератак // Современные средства связи. 2024. Т. 1, № 1. С. 67–71. EDN NIJUDK.

Baranovsky O. K. Particular indicators of the effectiveness of protection of information infrastructure objects from cyberattacks // Modern means of communication. 2024. Vol. 1, No. 1. P. 67–71. EDN NIJUDK. (In Russian).

[Бас21] Басан Е. С. Система самодиагностики для обнаружения кибератак на БПЛА на основе анализа изменения параметров: отчёт по проекту РНФ № 21-79-00194. 2021–2023.

Basan E. S. Self-diagnosis system for detecting cyber attacks on UAVs based on analysis of parameter changes: report on RSF project No. 21-79-00194. 2021–2023. (In Russian).

[Гур24] Гурчинский М. М., Тебуева Ф. Б. Обнаружение нарушителя агентами роевых робототехнических систем в условиях недетерминированной среды функционирования // СИИТ. 2024. Т. 6, № 3(18). С. 71-82. EDN AUVYOX.

Gurchinsky M. M., Tebueva F. B. Detection of an intruder by agents of swarm robotic systems in a non-deterministic operating environment // SIIT. 2024. Vol. 6, No. 3(18). P. 71-82. EDN AUVYOX. (In Russian).

[Кор23] Корчагин П. В., Кириенко А. Б. и др. Подход к комплексной вероятностной оценке защищённости информации от несанкционированного доступа в информационной системе критического назначения // Защита информации. Инсайд. 2023. № 6 (114). С. 14–21. EDN WFYRTU.

Korchagin P. V., Kiriyenko A. B., et al. An approach to a comprehensive probabilistic assessment of information security from unauthorized access in a critical information system // Information Security. Inside. 2023. No. 6 (114). P. 14–21. EDN WFYRTU. (In Russian).

[Мак20а] Макаренко С. И. Противодействие беспилотным летательным аппаратам. СПб.: Наукоёмкие технологии, 2020. 204 с. EDN YSBRZJ.

Makarenko S. I. Counteracting Unmanned Aerial Vehicles. St. Petersburg: Science-Intensive Technologies, 2020. EDN YSBRZJ. (In Russian).

[Мак20б] Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный аппарат как объект обнаружения и

Makarenko S. I., Timoshenko A. V., Vasilchenko A. S. Analysis of means and methods of countering unmanned aerial vehicles. Part 1. Unmanned aerial vehicle as an object of detection and destruction // Control, Communications

поражения // Системы управления, связи и безопасности. 2020. № 1. С. 109-146. EDN YIBMFH.

and Security Systems. 2020. No. 1. P. 109-146. EDN YIBMFH. (In Russian).

[Пет26] Петренко В. И., Тебуева Ф. Б., Соболева П. А. Метод доверенной оркестрации роботизированных агентов в децентрализованных средах на основе глубокого обучения с подкреплением // СИИТ. 2026. Т. 8, № 1(25). С. 75-87. EDN EMOZKB.

Petrenko V. I., Tebueva F. B., Soboleva P. A. Method of trusted orchestration of robotic agents in decentralized environments based on deep reinforcement learning // SIIT. 2026. Vol. 8, No. 1(25). P. 75-87. EDN EMOZKB. (In Russian).

[Саи25] Саитова Г. А., Габдуллина Э. Р. Методика определения проективного покрытия полей на основе дистанционного мониторинга // СИИТ. 2025. Т. 7, № 2(21). С. 48-55. EDN XTKJHQ.

Saitova G. A., Gabdullina E. R. Methodology for determining the projective coverage of fields based on remote monitoring // SIIT. 2025. T. 7, No. 2(21). pp. 48-55. EDN XTKJHQ. (In Russian).

[Скр24a] Скрыль С. В., Ицкова А. А., Ушаков К. Е. О возможности совершенствования процедур количественной оценки защищённости информации объектов критической информационной инфраструктуры от угроз несанкционированного доступа // Безопасность информационных технологий. 2024. Т. 31, № 3. С. 94–104. EDN CZFYYR.

Skryl S. V., Itskova A. A., Ushakov K. E. On the possibility of improving the procedures for quantitative assessment of the security of information of critical information infrastructure objects from threats of unauthorized access // Information Technology Security. 2024. Vol. 31, No. 3. P. 94–104. EDN CZFYYR. (In Russian).

[Скр24b] Скрыль С. В., Федюнин П. А. и др. Обоснование показателя для оценки управляемости защищённостью информации в автоматизированных системах управления критических приложений от воздействия вредоносного программного обеспечения // Безопасность информационных технологий. 2024. Т. 31, № 2. С. 30–41. EDN JHDZWS.

Skryl S. V., Fedyunin P. A. et al. Justification of an indicator for assessing the manageability of information security in automated control systems for critical applications from the impact of malicious software // Information Technology Security. 2024. Vol. 31, No. 2. pp. 30–41. EDN JHDZWS. (In Russian).

[Тра24] Трапезников Е. В., Магазев А. А., Касенов А. А. Марковская модель кибератак и ее применение к анализу защищенности информации в автоматизированных системах // МОИТ. 2024. Т. 12, № 2(45). EDN ZEEVLY.

Trapeznikov E. V., Magazev A. A., Kasenov A. A. Markov model of cyber attacks and its application to the analysis of information security in automated systems // MOIT. 2024. Vol. 12, No. 2(45). EDN ZEEVLY. (In Russian).

[Хал25] Халилов Р. Д., Муслимов Т. З. Сравнение моделей нейронных сетей для автоматического управления полетом квадрокоптера по заданной траектории // СИИТ. 2025. Т. 7, № 5(24). С. 86-108. EDN AMLCRV.

Khalilov R. D., Muslimov T. Z. Comparison of neural network models for automatic control of a quadcopter flight along a given trajectory // SIIT. 2025. Vol. 7, No. 5(24). P. 86-108. EDN AMLCRV. (In Russian).

ОБ АВТОРЕ | ABOUT THE AUTHOR

ВОЛОШИН Денис Геннадиевич
Северо-Кавказский федеральный университет, Россия.
ultrageron@gmail.com ORCID: 0009-0007-4841-0147.
Мл. науч. сотр. Иссл. в обл. информационной безопасности киберфизических систем.

VOLOSHIN Denis Gennadievich
North Caucasus Federal University, Russia.
ultrageron@gmail.com ORCID: 0009-0007-4841-0147.
Junior Research Fellow. Research in the area of information security of cyber-physical systems.

МЕТАДАННЫЕ | METADATA

Заглавие: Методика интегральной количественной оценки защищённости навигационной информации беспилотных летательных аппаратов лёгкого класса в условиях деструктивного воздействия.

Title: Methodology for the integrated quantitative assessment of the security of navigation information of light unmanned aerial vehicles under destructive impact conditions

Авторы: Волошин Д. Г.

Authors: Voloshin D. G.

Аннотация: Целью исследования является разработка методики количественной оценки защищённости навигационной информации беспилотных летательных аппаратов (БПЛА) лёгкого класса, дающую единый численный показатель и учитывающую ресурсные и эксплуатационные ограничения платформы. Методика опирается на вероятностно-рисковый подход: для каждой пары «угроза – уязвимость» вычисляется риск эксплуатации с учётом вероятности обнаружения угрозы, условной вероятности успешной эксплуатации, эффективности наиболее сильной применимой меры защиты и коэффициента критичности подсистемы; частные риски агрегируются во взвешенный интегральный показатель защищённости, корректируемый адаптивными коэффициентами электромагнитной обстановки, географии и интенсивности

Abstract: The aim of the research is to develop a methodology for the quantitative assessment of navigation information security for light-class unmanned aerial vehicles (UAVs), which provides a single numerical indicator and takes into account the platform's resource and operational constraints. The methodology is based on a probabilistic risk approach: for each "threat – vulnerability" pair, the exploitation risk is calculated considering the probability of threat detection, the conditional probability of successful exploitation, the effectiveness of the strongest applicable security measure, and the subsystem criticality coefficient; partial risks are aggregated into a weighted integral security indicator, adjusted by adaptive coefficients for the electromagnetic environment, geography, and attack intensity. The validity is confirmed by comparison with the NIST SP 800-30 methodology and expert validation. Using a light-class quadcopter weighing up to

атак. Достоверность подтверждена сопоставлением с методикой NIST SP 800-30 и экспертной валидацией. На примере квадрокоптера лёгкого класса массой до 25 кг интегральный показатель защищённости при базовой конфигурации составил 0,329 (низкий уровень) и возрос до 0,894 (высокий уровень) при полном наборе из шести мер защиты. Наибольший вклад в суммарный риск (около 59,6 %) вносит скрытый GPS-спуфинг. Для бюджетного ограничения 40 тыс. руб. найдено оптимальное подмножество мер, обеспечивающее показатель 0,822 при стоимости 35 тыс. руб. Учёт реальных условий эксплуатации снижает эффективную защищённость до 0,48-0,53. Предложенная методика обеспечивает сопоставимую количественную оценку альтернативных конфигураций защиты лёгких БПЛА и применима на этапах проектирования, модернизации и планирования миссии. Практическая значимость состоит в возможности обоснованного выбора набора мер защиты в условиях ограничений по стоимости и энергопотреблению.

Ключевые слова: Беспилотный летательный аппарат; оценка защищённости; интегральный показатель; вероятностный подход; GPS-спуфинг; риск эксплуатации уязвимостей; адаптивные коэффициенты среды; оптимизация мер защиты.

Язык: Русский.

Статья поступила в редакцию 22 июня 2026 г.

25 kg as an example, the integral security indicator for the baseline configuration was 0.329 (low level) and increased to 0.894 (high level) with a full set of six security measures. The greatest contribution to the total risk (about 59.6%) is made by covert GPS spoofing. For a budget constraint of 40,000 rubles, an optimal subset of measures was found, providing an indicator of 0.822 at a cost of 35,000 rubles. Consideration of actual operating conditions reduces the effective security to 0.48–0.53. The proposed methodology provides a comparable quantitative assessment of alternative security configurations for light UAVs and is applicable at the stages of design, upgrade, and mission planning. The practical significance lies in the possibility of a substantiated selection of a set of security measures under cost and power consumption constraints.

Key words: Unmanned aerial vehicle; security assessment; integral indicator; probabilistic approach; GPS spoofing; vulnerability exploitation risk; adaptive environmental factors; security measures optimization.

Language: Russian.

The article was received by the editors on 22 June 2026.