УДК 629.7
DOI: 10.26467/2079-0619-2025-28-4-40-49

Математическая модель угроз авиационной сети передачи данных в условиях несанкционированного вмешательства

А.А. Ганичев[1], В.И. Петров[1]
[1]Московский государственный технический университет гражданской авиации, г. Москва, Россия

Аннотация: В связи с возрастающей степенью интеграции бортовых и наземных сетей передачи данных в авиации и ростом количества информационных угроз все более необходимой становится разработка моделей, позволяющих проводить комплексную оценку защищенности таких систем от несанкционированного вмешательства. Одним из перспективных направлений повышения устойчивости авиационных сетей является создание математических моделей, позволяющих учитывать не только технические сбои и случайные отказы оборудования, но и преднамеренные атаки нарушителей. В работе предложена математическая модель угроз авиационной сети передачи данных, выполненная в соответствии с рекомендациями ИКАО и требованиями стандартов ARINC. Представление структуры сети осуществляется в виде ориентированного графа, узлы и ребра которого характеризуются вероятностными показателями отказов и подверженностью атакам. Особенностью разработанной модели является объединение вероятностных характеристик случайных отказов оборудования и сценариев целенаправленных атак, а также параметров эффективности функционирования систем обнаружения несанкционированного вмешательства. На основе подходов теории вероятностей синтезирован алгоритм, позволяющий рассчитывать интегральный показатель риска потери связности сети и деградации ее характеристик. Отличительная особенность алгоритма заключается в том, что он позволяет одновременно учитывать различные типы воздействий и производить количественную оценку уязвимости элементов сети. Выполнено численное моделирование предложенной модели, представлены результаты оценки критичности отдельных узлов сети и каналов передачи данных. Анализ результатов показал, что применение разработанной математической модели позволяет обоснованно определять наиболее уязвимые компоненты авиационной сети и выбирать адекватные меры защиты.

Ключевые слова: несанкционированное вмешательство, авиационная сеть передачи данных, надежность сети, связность, обнаружение атак, риск, модель угроз.

Для цитирования: Ганичев А.А., Петров В.И. Математическая модель угроз авиационной сети передачи данных в условиях несанкционированного вмешательства // Научный вестник МГТУ ГА. 2025. Т. 28, № 4. С. 40–49. DOI: 10.26467/2079-0619-2025-28-4-40-49

Mathematical model of threats to an aviation data network under unauthorized access

A.A. Ganichev[1], V.I. Petrov[1]
[1]Moscow State Technical University of Civil Aviation, Moscow, Russia

Abstract: Due to the increasing integration of onboard and ground-based data networks in aviation and the associated rise in information threats, the development of comprehensive models capable of assessing the security of such systems against unauthorized access is becoming increasingly necessary. One promising direction for enhancing the resilience of aviation networks is the creation of mathematical models that consider not only technical malfunctions and random equipment failures but also deliberate cyberattacks by intruders. This paper proposes a mathematical model of threats to aviation data networks, developed in accordance with ICAO recommendations and the requirements of ARINC standards. The network structure is represented as a directed graph, the nodes and edges of which are characterized by probabilistic indicators of failures and vulnerability to attacks. A distinctive feature of the developed model is the integration of probabilistic characteristics of random equipment failures, intentional attack scenarios, and parameters reflecting the efficiency of systems detecting unauthorized access. Utilizing

probabilistic theory approaches, we synthesized an algorithm enabling the calculation of an integral indicator representing the risk of network connectivity loss and performance degradation. A significant aspect of this algorithm is its ability to simultaneously account for various types of threats and quantitatively assess the vulnerability of network elements. Numerical simulations of the proposed model were conducted, and results evaluating the criticality of specific network nodes and data transmission channels are presented. The analysis confirmed that applying the developed mathematical model provides a sound basis for identifying the most vulnerable aviation network components and selecting appropriate protective measures.

Key words: unauthorized interference, aviation data network, network reliability, connectivity, attack detection, risk, threat model.

For citation: Ganichev, A.A., Petrov, V.I. (2025). Mathematical model of threats to an aviation data network under unauthorized access. Civil Aviation High Technologies, vol. 28, no. 4, pp. 40–49. DOI: 10.26467/2079-0619-2025-28-4-40-49

Введение

Обеспечение защиты сетей авиационного транспорта от несанкционированного вмешательства (НСВ) приобретает первостепенную важность в условиях цифровизации авиационной отрасли[1]. Переход авиационных систем связи от аналоговой голосовой связи к использованию IP-сетей передачи данных значительно расширяет их функциональные возможности, однако сопровождается существенным увеличением числа киберугроз[2], способных нарушить работу бортовых комплексов и систем управления полетом [1–3]. Кроме того, внедрение технологий интернета вещей и других интеллектуальных технологий в авиационную инфраструктуру расширяет поверхность атаки и приводит к появлению дополнительных уязвимостей [4, 5]. НСВ в авиационную деятельность может проявляться в искажении координат воздушного судна, передаче ложных команд экипажу, блокировке каналов связи или создании помех, препятствующих обмену критически важными данными [2, 6]. Эти риски требуют разработки дополнительных мер защиты, направленных на обеспечение надежности авиационных систем и предотвращение дестабилизации управления воздушным движением [7–9].

В последние годы проведен ряд исследований, посвященных повышению защиты от НСВ на воздушном транспорте: их тематика охватывает широкий спектр направлений, от организационных мер в аэропортах [10] и создания комплексных бортовых систем безопасности [7, 11] до моделирования несанкционированного воздействия на авиационные системы [12, 13] и использования методов машинного обучения для обнаружения вторжений [14–16]. Однако предлагаемые в этих работах подходы остаются фрагментарными и не охватывают весь спектр актуальных угроз для авиационных сетей передачи данных [17, 18]. Также отраслевые стандарты и рекомендации (например, ИКАО и IATA) зачастую не успевают за быстрым развитием методов проведения НСВ, а существующие подходы к оценке рисков и тестированию показывают, что имеющиеся средства защиты не покрывают всех возможных сценариев атак [6, 19].

Современные исследования подтверждают наличие широкого спектра уязвимостей в архитектуре авиационных сетей передачи данных. Нарушители способны искажать маршрутную информацию, перехватывать управляющие сигналы и нарушать функционирование взаимодействующих подсистем. В беспилотных авиационных системах, как показано в [20, 21], не реализованы устойчивые механизмы противодействия несанкционированному вмешательству. Зафиксированы случаи внедрения вредоносных модификаций, перехвата элементов управления и деструктивного воздействия на навигационные блоки.

Отсутствие формализованных подходов существенно затрудняет оценку устойчивости авиационных сетей передачи данных. В [22] предложена лабораторная платформа, ориентированная на воспроизведение реаль-

[1] Compilation of Cyber Security Regulations, Standards, and Guidance [Электронный ресурс] // IATA. 2022. URL: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf (дата обращения: 20.11.2024).

[2] Security and facilitation strategic objective: Aviation cybersecurity strategy // ICAO, 2019. 8 p.

ных сценариев атак, в том числе с применением SDR и анализа межсистемных взаимодействий. В [23] систематизированы типовые уязвимости сетевых доменов воздушных судов, продемонстрированы ошибки в логической изоляции подсистем и слабость штатных средств защиты.

Вместе с тем до настоящего времени отсутствовала формализованная модель, позволяющая количественно оценить влияние как случайных отказов оборудования, так и преднамеренных атак нарушителей на связность авиационной сети. Настоящая работа нацелена на восполнение этого пробела за счет разработки интегрированной математической модели угроз.

Методы

При разработке модели применены рекомендации отраслевых стандартов по авиационной безопасности: использована классификация каналов связи согласно ARINC 811[3] (разделение на защищенные и незащищенные каналы) и учтены методические положения RTCA DO-356A[4] при анализе сценариев вмешательства. В соответствии с этим сеть передачи данных (СПД) представляется как граф узлов и соединений, для которого проводится вероятностный анализ надежности. Каждый узел и канал модели характеризуется вероятностями безотказной работы и отказа, определяемыми на основе статистических данных и допущения о независимости отказов. В модель вводятся угрозы несанкционированного вмешательства – преднамеренные воздействия на узлы и линии связи, – которые рассматриваются как дополнительные вероятностные факторы отказа элементов сети.

Такой подход, основанный на теории надежности сетей и анализе минимальных уязвимых наборов компонентов, позволяет формализовать задачу обеспечения устойчивости авиационной сети к несанкционированному вмешательству в виде совокупности вероятностных показателей. Далее представлена разработанная модель.

Разработка математической модели

Для начала формализуем структуру авиационной СПД. Будем представлять сеть в виде графа G с множеством узлов V и ребер E:

$$G = (V, E). \quad (1)$$

Здесь V – множество узлов (вершин) графа, а E – множество соединений (ребер) между ними.

Узлами графа выступают бортовые и наземные вычислительные устройства (бортовые компьютеры воздушного судна, серверы центров управления, ретрансляторы и т. д.). Ребра графа соответствуют каналам передачи данных (радиолиниям, спутниковым каналам и пр.), обеспечивающим связь между узлами. Предполагается, что топология графа фиксирована в рассматриваемый период, то есть состав узлов и наличие каналов задано изначально и не изменяется с течением времени.

Каждый элемент сети обладает определенной надежностью и, соответственно, ненулевой вероятностью отказа. Введем обозначения: пусть p_i – вероятность безотказной работы узла i в рассматриваемом периоде. Тогда можно выразить:

$$q_i = 1 - p_i, \quad (2)$$

где q_i – вероятность отказа этого узла по техническим причинам.

Аналогично для каждого канала связи (ребра) $e \in E$ обозначим через p_e вероятность его исправного функционирования:

[3] ARINC Project Paper 658. Internet protocol suite (IPS) for aeronautical safety services roadmap document [Электронный ресурс] // ARINC Project Paper 658, 2017. 15 p. URL: https://www.icao.int/APAC/Meetings/2017%20ACSICG4/IP05_USA%20AI.3%20-%20IPS%20Roadmap.pdf (дата обращения: 20.11.2024).

[4] RTCA DO-356. Airworthiness security methods and consideration [Электронный ресурс] // GlobalSpec, 2018. 370 p. URL: https://standards.globalspec.com/std/10398650/rtca-do-356 (дата обращения: 20.11.2024).

$$q_e = 1 - p_e, \quad (3)$$

где q_e – вероятность отказа канала.

Примем упрощающее предположение, что отказы отдельных узлов и каналов являются статистически независимыми событиями (в реальности могут наблюдаться коррелированные сбои, но независимость допускается для облегчения анализа).

Для оценки работоспособности всей сети введем понятие связности графа. Сеть считается связной и функционирующей, если для любой пары важных узлов (например, «борт – центр управления») существует хотя бы один путь, соединяющий их посредством исправных узлов и каналов. Событие нарушения связности, напротив, означает, что найдется хотя бы одна пара узлов, между которыми не осталось ни одного работоспособного маршрута передачи данных. Вероятность сохранения связности сети можно рассматривать как показатель ее общей надежности. Вычисление этой вероятности эквивалентно задаче оценки надежности графа с заданными надежностями элементов.

В общем случае точное вычисление вероятности связности для произвольного графа представляет трудность, поскольку требует учета всех возможных комбинаций отказов элементов. Однако для некоторых типовых конфигураций сети можно записать аналитические выражения. Например, если два важных узла соединены между собой последовательной цепочкой из n-каналов, то сеть останется связной только при работоспособности каждого из этих каналов. В таком случае вероятность сохранения связи между узлами определяется произведением надежностей каналов:

$$R_{conn} = \prod_{e=1}^{N} p_e. \quad (4)$$

Напротив, при наличии резервирования каналов (параллельных независимых линий связи) надежность сети возрастает. Для случая двух параллельных каналов между одними и теми же узлами вероятность того, что связь **полностью** потеряна, равна произведению вероятностей отказа каждого канала. Соответственно, вероятность сохранения связи хотя бы по одному из двух каналов запишется как

$$R_{conn} = 1 - (1 - p_1)(1 - p_2). \quad (5)$$

Приведенные упрощенные примеры иллюстрируют, как топология сети влияет на ее надежность: наличие альтернативных маршрутов (дублирующих узлов или каналов) снижает вероятность полного отказа связи. В реальной авиационной сети структура может быть более сложной, включать множество узлов и пересекающихся маршрутов. Для общей модели введем множество минимальных разрезов графа – критических наборов компонентов, отказ которых приводит к нарушению связности. Обозначим через C множество всех минимальных разрезов:

$$C = \{C_1, C_2, \dots, C_K\}, \quad (6)$$

где каждый C_i представляет собой минимальное множество узлов и (или) ребер, при одновременном выходе из строя которых граф G распадается на несвязные части. Таким образом, элементы C_i – это «критические» узлы и линии, образующие уязвимое место сети.

Авиационная СПД подвержена не только случайным сбоям, но и целенаправленным несанкционированным воздействиям. К ним относятся атаки на узлы сети (например, несанкционированное проникновение в бортовую сеть или вывод из строя сервера управления), преднамеренные помехи в каналах связи (глушение радиосигнала), внедрение ложных команд или данных и другие виды злоумышленных действий, способных нарушить нормальную работу системы. Для количественного анализа подобных угроз введем их вероятностную модель. Предположим, что для каждого элемента сети можно оценить вероятность успешной атаки в рассматриваемый период. Обозначим через P_i^{attack} вероятность того, что узел $i \in V$ будет скомпрометирован злоумышленником, то есть подвергнется атаке, нарушающей его функцио-

нирование. Аналогично для канала $e \in E$ введем P_e^{attack} – вероятность того, что на канал e будет совершена успешная атака. Как правило, величины P_i^{attack} относительно невелики, но отличны от нуля, что отражает саму возможность успешного осуществления атаки при определенных условиях.

НСВ, по сути, приводит к выводу узла или канала из строя аналогично техническому отказу, хотя и имеет иную природу. Поэтому естественно рассматривать атаку как дополнительную причину отказа компонента. Объединим две причины нарушения работы – случайный отказ и успешную атаку – в единой вероятностной модели элемента сети. Если считать эти причины статистически независимыми, то итоговая вероятность того, что компонент i выйдет из строя (либо из-за отказа, либо в результате атаки), определяется выражением

$$q_j^{total} = 1 - \big(1 - q_j\big)\big(1 - P_j^{attack}\big). \qquad (7)$$

Здесь q_j^{total} – суммарная вероятность неработоспособности элемента i по любой из двух причин. Формула (7) показывает, что элемент выйдет из строя, если произойдет хотя бы одно из двух событий: внутренний технический сбой или успешное внешнее воздействие. Эквивалентно можно записать вероятность безотказной работы с учетом атак:

$$p_j^{total} = (1 - q_j)(1 - P_j^{attack}), \qquad (8)$$

то есть компонент продолжит функционировать только при отсутствии отказа и отсутствии успешной атаки.

Вероятности P_j^{attack} характеризуют уязвимость элементов сети. Злоумышленник, как правило, стремится атаковать наиболее критичные узлы и линии связи, вывод из строя которых приводит к максимальному нарушению работы сети. В терминах введенных ранее минимальных разрезов целенаправленная атака может быть нацелена на выведение из строя всех компонентов некоторого разреза C_K, что гарантированно нарушит связность сети. Однако возможность реализации такой комплексной атаки зависит от ресурсов нарушителя и снижается, если разрез включает значительное число элементов. Тем не менее математическая модель должна учитывать различные сценарии атак: от одиночных воздействий на отдельные узлы или каналы до комбинированных атак, нацеленных на несколько элементов сети одновременно. Для каждого сценария можно задать соответствующую вероятность реализации угрозы P_j^{attack} или группы вероятностей для набора атакуемых элементов.

Важным фактором, снижающим влияние угроз, является работающая в сети система обнаружения НСВ. Предположим, что в рассматриваемой авиационной СПД внедрены средства мониторинга и диагностики, позволяющие выявлять аномалии в передаче данных. К таким средствам относятся системы обнаружения атак, анализаторы сетевого трафика, механизмы контроля целостности сообщений и другие технологии мониторинга. Их основная задача – своевременное выявление фактов атаки или аномального поведения сети с высокой вероятностью при минимальном числе ложных тревог.

Смоделируем процесс выявления атак в вероятностной постановке. Введем два ключевых показателя эффективности системы обнаружения:

(1) p_d – вероятность правильного обнаружения атаки (чувствительность системы);

(2) p_{fa} – вероятность ложного срабатывания, то есть формирования сигнала тревоги при отсутствии реальной угрозы.

Если в СПД происходит атака, то с вероятностью p_d она будет зафиксирована средствами мониторинга, а с вероятностью $1 - p_d$ атака останется незамеченной. Значение p_d, близкое к 1, означает эффективное обнаружение практически всех атак, тогда как снижение p_d указывает на возрастание вероятности пропуска угроз. Показатель p_{fa} характеризует избирательность системы: при отсутствии атак ложные срабатывания происходят с вероятностью p_{fa}. Желательно, чтобы p_{fa} был минимальным, во избежание

избыточной нагрузки на операторов и системы реагирования на инциденты.

Таким образом, вероятность успешной атаки, не обнаруженной средствами мониторинга, уменьшается пропорционально фактору обнаружения p_d. Формально введем эффективную вероятность успешной атаки с учетом работы системы обнаружения:

$$\tilde{P}_j^{attack} = P_j^{attack}(1 - p_d). \quad (9)$$

Подставляя $\tilde{P}_j^{attack}$ вместо P_j^{attack} в формулу (7) для вероятности отказа компонента, можно пересчитать итоговую вероятность его неработоспособности с учетом функционирования системы мониторинга. Из (7) с учетом (9) получаем для любого узла или канала

$$\tilde{q}_i = 1 - (1 - q_j)(1 - \tilde{P}_j^{attack}), \quad (10)$$

где q_j – вероятность технического отказа узла или канала j;

$\tilde{P}_j^{attack}$ – вероятность успешной необнаруженной атаки на компонент j.

Определенные выше величины позволяют оценить совокупный риск для СПД. Будем понимать под риском $P(F)$ вероятность события F, при котором сеть теряет связность, то есть обмен данными между некоторыми узлами становится невозможен. Такое событие F наступает, если выйдут из строя все компоненты по крайней мере одного из минимальных разрезов C_K графа сети. Вероятность нарушения связности, таким образом, определяется комбинацией независимых отказов и необнаруженных атак, затрагивающих узлы и каналы сети. Предполагая независимость таких исходов для разных разрезов, можно получить приближенную оценку общей вероятности F как сумму вероятностей отказа всех критических наборов:

$$P(F) = \sum_{k=1}^{K} \prod_{j \in C_K} \tilde{q}_i. \quad (11)$$

Формула (11) учитывает все возможные критические разрезы сети и, по сути, складывает риски потери связности по каждому из них. Эта сумма несколько завышает истинное значение $P(F)$, так как различные разрезы могут иметь общие компоненты (события их отказа не независимы). Для более точного расчета потребовалось бы применение принципа включений-исключений или других методов теории надежности сетей. Тем не менее полученное выражение дает полезную оценку риска и позволяет сравнивать различные конфигурации сети и варианты защитных мероприятий.

Если какой-либо разрез сети имеет существенно более высокую вероятность отказа по сравнению с остальными, то общий риск $P(F)$ определяется в первую очередь этим «слабым местом». Например, если в сети существует единственный критически важный узел, через который проходят все данные, то вероятность полного отказа сети приближенно равна $\tilde{q}_i$ – эффективной вероятности выхода из строя данного узла (с учетом атак). В более сбалансированных сетях, где отказ отдельного элемента не приводит сразу к распаду сети, в расчет риска вносят вклад несколько слагаемых в (11).

Обсуждение результатов

Полученная математическая модель позволяет количественно оценить влияние отказов и несанкционированных воздействий на функционирование авиационной СПД. На основании модели можно выявить наиболее уязвимые элементы сети – узлы и каналы, входящие в минимальные разрезы с наибольшей вероятностью отказа. Очевидно, что именно отказ этих критичных компонентов определяет основной вклад в риск $P(F)$. Следующим этапом после оценки риска является разработка мер по его снижению. Оптимизация стратегии защиты авиационной сети должна быть направлена на уменьшение вероятностей успешных атак и отказов тех элементов, которые наиболее существенно влияют на связность сети, что будет отражено в будущих публикациях.

Заключение

В работе представлена математическая модель, описывающая угрозы функционированию авиационной СПД в условиях несанкционированного вмешательства. Предложенный подход интегрирует вероятностную модель технических отказов с моделью преднамеренных атак и их обнаружения. На основе модели получены аналитические выражения для оценки вероятности потери связности сети (формулы (7)–(11)) и показано, как различные факторы – топология сети, надежность узлов, интенсивность атак и эффективность их обнаружения – влияют на суммарный риск нарушения работы. Научная новизна результата состоит в формальном учете факторов несанкционированного воздействия и мониторинга безопасности в задаче надежности сети. Практическая ценность работы заключается в том, что модель позволяет выявить наиболее уязвимые элементы сети и обосновать приоритетные меры защиты. Повышение надежности критических узлов и каналов, а также внедрение эффективных систем обнаружения НСВ снижает вероятность успешных атак и тем самым повышает безопасность полетов. Разработанная модель может быть использована при проектировании перспективных информационных СПД для количественной оценки риска вмешательства и оптимального распределения ресурсов защиты.

Список литературы

1. **Ukwandu E., Ben-Farah M.A., Hindy H. и др.** Cyber-security challenges in aviation industry: a review of current and future trends [Электронный ресурс] // Information. 2022. Vol. 13, no. 3. ID: 146. DOI: 10.3390/info13030146 (дата обращения: 20.11.2024).

2. **Ben Mahmoud M.S., Pirovano A., Larrieu N.** Aeronautical communication transition from analog to digital data: A network security survey // Computer Science Review. 2014. Vol. 11–12. Pp. 1–29. DOI: 10.1016/j.cosrev.2014.02.001

3. **Kızılcan S., Mızrak K.C.** Cyber attacks in civil aviation and the concept of cyber security // International Journal of Disciplines Economics & Administrative Sciences Studies. 2022. Vol. 8, no. 47. Pp. 742–752. DOI: 10.29228/ideas.65891

4. **Gaurav D.** Cyber security challenges in aviation communication, navigation, and surveillance / D. Gaurav, Ch. Gaurav, S. Vikas, Y. Ilsun, R.Ch. Kim-Kwang [Электронный ресурс] // Computers & Security. 2022. Vol. 113. ID: 102516. DOI: 10.1016/j.cose.2021.102516 (дата обращения: 20.11.2024).

5. **Kagalwalla N., Churi P.P.** Cybersecurity in aviation: An intrinsic review [Электронный ресурс] // 2019 5th International Conference On Computing, Communication, Control and Automation (ICCUBEA). India, Pune, 2019. Pp. 1–6. DOI: 10.1109/ICCUBEA47591.2019.9128483 (дата обращения: 20.11.2024).

6. **Corretjer P.J.** A Cybersecurity analysis of today's commercial aircrafts and aviation industry systems: A thesis master of science. USA, NY, Utica College, 2018. 22 p.

7. **Кулик А.А., Большаков А.А.** Методологические подходы к разработке интеллектуальной авиационной системы управления безопасностью полетов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2021. № 3. С. 41–48. DOI: 10.24143/2072-9502-2021-3-41-48

8. **Basora L., Olive X., Dubot T.** Recent advances in anomaly detection methods applied to aviation [Электронный ресурс] // Aerospace. 2019. Vol. 6, no. 11. ID: 117. DOI: 10.3390/aerospace6110117 (дата обращения: 20.11.2024).

9. **Zhang R.** Analysis of message attacks in aviation data-link communication / R. Zhang, G. Liu, J. Liu, J.P. Nees [Электронный ресурс] // IEEE Access. 2018. Vol. 6. Pp. 455–463. DOI: 10.1109/ACCESS.2017.2767059 (дата обращения: 20.11.2024).

10. **Мешанков Д.М., Тихонов А.И.** Внедрение новой информационной системы обеспечения безопасности полетов [Электронный ресурс] // Московский экономический журнал. 2021. № 10. DOI: 10.24411/

2413-046X-2021-10601 (дата обращения: 20.11.2024).

11. Коптев Д.С., Мухин И.Е. Концепция разработки комплексных бортовых систем обеспечения безопасности полетов воздушных судов, включая системы контроля функционального состояния оператора // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14, № 12. С. 58–65. DOI: 10.36724/2072-8735-2020-14-12-58-65

12. Ганичев А.А., Пителинский К.В., Бритвина В.В. Статистический анализ потенциальных угроз информационной безопасности в бортовой сети воздушного судна // Вопросы защиты информации. 2024. № 1 (144). С. 11–22. DOI: 10.52190/2073-2600_2024_1_11

13. Петров В.И. Недекларированные возможности программного обеспечения бортовых компьютеров воздушного судна // Гражданская авиация на современном этапе развития науки, техники и общества: сборник тезисов докладов Международной научно-техн. конференции, посвященной 45-летию Университета. Москва, 18–20 мая 2016 года. М.: ИД Академии имени Н.Е. Жуковского, 2016. С. 160.

14. Taleqani A.R. Machine learning approach to cyber security in aviation / A.R. Taleqani, K.E. Nygard, R. Bridgelall, J. Hough // 2018 IEEE International Conference on Electro/Information Technology (EIT). USA, MI, Rochester, 2018. Pp. 0147–0152. DOI: 10.1109/EIT.2018.8500165

15. Wrana M.M. OD1NF1ST: True skip intrusion detection and avionics network cyber-attack simulation / M.M. Wrana, M. Elsayed, K. Lounis, Z. Mansour, S. Ding, M. Zulkernine [Электронный ресурс] // ACM Transactions on Cyber-Physical Systems. 2022. Vol. 6, no. 4. ID: 33. 27 p. DOI: 10.1145/3551893 (дата обращения: 20.11.2024).

16. Машошин А.О. Определение истинности сообщений системы автоматического зависимого наблюдения в условиях несанкционированного вмешательства на управление воздушным движением за счет метода монолатерации // Научный вестник ГосНИИ ГА. 2021. № 37. С. 136–145.

17. Ганичев А.А. Модель угроз несанкционированного вмешательства в беспроводных информационных системах авионики / А.А. Ганичев, К.В. Пителинский, С.А. Кесель, В.А. Пиков // Вопросы защиты информации. 2024. № 4 (147). С. 35–43. DOI: 10.52190/2073-2600_2024_4_35

18. Петров В.И. Методика анализа программного обеспечения бортовых компьютеров воздушного судна на отсутствие недекларированных возможностей сигнатурно-эвристическим способом // Научный вестник МГТУ ГА. 2017. Т. 20, № 1. С. 186–193.

19. Kessler G.C., Craiger J.P. Aviation cybersecurity: An overview [Электронный ресурс] // The National Training Aircraft Symposium (NTAS) 2018. URL: https://commons.erau.edu/ntas/2018/presentations/37/ (дата обращения: 20.11.2024).

20. Исрафилов А. Современные вызовы в области кибербезопасности беспилотных авиационных систем [Электронный ресурс] // Universum: технические науки. 2024. № 2 (119). URL: https://7universum.com/ru/tech/archive/item/16760 (дата обращения: 20.11.2024).

21. Лянгузов Д.А., Плюснин Н.И. Безопасность и уязвимость сетей беспилотных летательных аппаратов: обзор // Известия ТулГУ. Технические науки. 2023. Вып. 7. С. 528–529. DOI: 10.24412/2071-6168-2023-7-528-529

22. Costin A. Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications / A. Costin, H. Turtiainen, S. Khandker, T. Hämäläinen [Электронный ресурс] // Cryptography and Security. 2023. DOI: 10.48550/arXiv.2302.08359 (дата обращения: 20.11.2024).

23. Habler E., Bitton R., Shabtai A. Evaluating the security of aircraft systems [Электронный ресурс] // Cryptography and Security. 2022. 38 p. DOI: 10.48550/arXiv.2209.04028 (дата обращения: 20.11.2024).

References

1. Ukwandu, E., Ben-Farah, M.A., Hindy, H. et al. (2022). Cyber-security challenges in aviation industry: a review of current and fu-

ture trends. *Information*, vol. 13, no. 3, ID: 146. DOI: 10.3390/info13030146 (accessed: 20.11.2024).

2. Ben Mahmoud, M.S., Pirovano, A., Larrieu, N. (2014). Aeronautical communication transition from analog to digital data: A network security survey. *Computer Science Review*, vol. 11–12, pp. 1–29. DOI: 10.1016/j.cosrev.2014.02.001

3. Kızılcan, S., Mızrak, K.C. (2022). Cyber attacks in civil aviation and the concept of cyber security. *International Journal of Disciplines Economics & Administrative Sciences Studies*, vol. 8, no. 47, pp. 742–752. DOI: 10.29228/ideas.65891

4. Gaurav, D., Gaurav, Ch., Vikas, S., Ilsun, Y., Kim-Kwang, R.Ch. (2022). Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, vol. 113. ID: 102516. DOI: 10.1016/j.cose.2021.102516 (accessed: 20.11.2024).

5. Kagalwalla, N., Churi, P.P. (2019). Cybersecurity in aviation: An intrinsic review. *In: 2019 5th International Conference On Computing, Communication, Control and Automation (ICCUBEA)*, India, Pune, pp. 1–6. DOI: 10.1109/ICCUBEA47591.2019.9128483 (accessed: 20.11.2024).

6. Corretjer, P.J. (2018). A Cybersecurity analysis of today's commercial aircrafts and aviation industry systems: A thesis master of science. USA, NY, Utica College, 22 p.

7. Kulik, A.A., Bolshakov, A.A. (2021). Methodological approaches to development of intelligent aviation safety control system. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, no. 3, pp. 41–48. DOI: 10.24143/2072-9502-2021-3-41-48 (in Russian)

8. Basora, L., Olive, X., Dubot, T. (2019). Recent advances in anomaly detection methods applied to aviation. *Aerospace*, vol. 6, no. 11, ID: 117. DOI: 10.3390/aerospace6110117 (accessed: 20.11.2024).

9. Zhang, R., Liu, G., Liu, J., Nees, J.P. (2018). Analysis of message attacks in aviation data-link communication. *IEEE Access*, vol. 6, pp. 455–463. DOI: 10.1109/ACCESS.2017.2767059 (accessed: 20.11.2024).

10. Meshankov, D.V., Tikhonov, A.I. (2021). Implementation of a new safety information system. *Moscow Economic Journal*, no. 10. DOI: 10.24411/2413-046X-2021-10601 (accessed: 20.11.2024). (in Russian)

11. Koptev, D.S., Mukhin, I.E. (2020). Concept of integrated airborne systems for providing aircraft operations safety, including systems for monitoring the functional state of the operator. *T-Comm*, vol. 14, no. 12, pp. 58–65. DOI: 10.36724/2072-8735-2020-14-12-58-65

12. Ganichev, A.A., Pitelinskiy, K.V., Britvina, V.V. (2024). Statistical analysis of potential threats to information security in the aircraft on-board network. *Information security questions*, no. 1 (144), pp. 11–22. DOI: 10.52190/2073-2600_2024_1_11 (in Russian)

13. Petrov, V.I. (2016). Undeclared Capabilities of Aircraft Onboard Computer Software. *In: Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva: sbornik tezisov dokladov Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, posvyashchennoy 45-letiyu Universiteta*, p. 160. (in Russian)

14. Taleqani, A.R., Nygard, K.E., Bridgelall, R., Hough, J. (2018). Machine learning approach to cyber security in aviation. *In: 2018 IEEE International Conference on Electro/Information Technology (EIT)*, Rochester, MI, USA, pp. 0147–0152. DOI: 10.1109/EIT.2018.8500165

15. Wrana, M.M., Elsayed, M., Lounis, K., Mansour, Z., Ding, S., Zulkernine, M. (2022). OD1NF1ST: True skip intrusion detection and avionics network cyber-attack simulation. *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 4, ID: 33, 27 p. DOI: 10.1145/3551893 (accessed: 20.11.2024).

16. Mashoshin, A.O. (2021). Message verification of the automatic dependent surveillance system under unauthorized intervention using the monolateration method. *Scientific Bulletin of the State Scientific Research Institute of Civil Aviation (GosNII GA)*, no. 37, pp. 136–145. (in Russian)

17. Ganichev, A.A., Pitelinskiy, K.V., Kesel, S.A., Pikov, V.A. (2024). Threat model of unauthorized interference in wireless avionics information systems. *Information security ques-*

tions, no. 4 (147), pp. 35–43. DOI: 10.521 90/2073-2600_2024_4_35 (in Russian)

18. Petrov, V.I. (2017). The technique of analysis of software of on-board computers of air vessel to absence of undeclared capabilities by signature-heuristic way. *Civil Aviation High Technologies*, vol. 20, no. 1, pp. 186–193. (in Russian)

19. Kessler, G.C., Craiger, J.P. (2018). Aviation cybersecurity: An overview. *In: The National Training Aircraft Symposium (NTAS) 2018*. Available at: https://commons.erau.edu/ntas/2018/presentations/37/ (accessed: 20.11.2024).

20. Israfilov, A. (2024). Contemporary challenges in cybersecurity of unmanned aerial systems. *Universum: Technical Sciences*, no. 2 (119). Available at: https://7universum.com/ru/tech/archive/item/16760 (accessed: 20.11.2024). (in Russian)

21. Lyanguzov, D.A., Plyusnin, N.I. (2023). Security and vulnerability of unmanned aerial vehicle networks: a review. *Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskiye nauki*, issue 7, pp. 528–529. DOI: 10.24412/2071-6168-2023-7-528-529 (in Russian)

22. Costin, A., Turtiainen, H., Khandker, S., Hämäläinen, T. (2023). Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications. *Cryptography and Security*. DOI: 10.48550/arXiv.2302.08359 (accessed: 20.11.2024).

23. Habler, E., Bitton, R., Shabtai, A. (2022). Evaluating the security of aircraft systems. *Cryptography and Security*, 38 p. DOI: 10.48550/arXiv.2209.04028 (accessed: 20.11.2024).

Сведения об авторах

Ганичев Александр Александрович, старший преподаватель кафедры основ радиотехники и защиты информации МГТУ ГА, alexunderlich@gmail.com.

Петров Виктор Иванович, кандидат технических наук, доцент, заведующий кафедрой основ радиотехники и защиты информации, декан факультета авиационных систем и комплексов МГТУ ГА, v.petrov@mstuca.ru.

Information about the authors

Alexandr A. Ganichev, Senior Lecturer, the Chair of Fundamentals of Radio Engineering and Information Security, Moscow State Technical University of Civil Aviation, alexunderlich@gmail.com.

Viktor I. Petrov, Candidate of Technical Sciences, Associate Professor, the Head of the Chair of Fundamentals of Radio Engineering and Information Security, the Dean of the Faculty of Aviation Systems and Complexes, Moscow State Technical University of Civil Aviation, v.petrov@mstuca.ru.

Поступила в редакцию	24.03.2025	Received	24.03.2025
Одобрена после рецензирования	30.04.2025	Approved after reviewing	30.04.2025
Принята в печать	24.07.2025	Accepted for publication	24.07.2025