АЗН-В и информационная безопасность воздушного движения

Э.Фальков, к.т.н., начальник отделения ФГУП "ГосНИИАС" / falkov@gosniias.ru,
С.Шаврин, д.т.н, профессор и начальник НИЛ 16 МТУСИ / sss@mtuci.ru

УДК 621.396, DOI: 10.22184/2070-8963.2020.90.5.50.56

Анализируется проблема информационной безопасности наблюдения за воздушным движением АЗН-В. Отмечается, что решение этой проблемы не исчерпывается обеспечением конфиденциальности, но включает также аутентификацию источника сообщений и связанную с ней неотрекаемость авторства источником сообщения, идентификацию целостности сообщений и контроль доступа, в том числе защиту от повторов "в записи" ранее переданных сообщений. Сделан вывод, что дальнейшее использование в целях АЗН-В системы сквиттера 1090 ES не соответствует современным требованиям безопасности воздушного движения и может стать в том числе весомым подспорьем для террористов. В качестве альтернативы предлагается реализация самоорганизующейся сетевой концепции АЗН-В на основе протокола VDL-4, поддерживающего необходимые для использования криптографических алгоритмов виды протоколов.

Одним из главных факторов обеспечения безопасности полетов воздушных судов (ВС) является полнота информации о положении ВС в воздушном пространстве – адекватная ситуационная осведомленность – как для органов управления воздушным движением, так и для его непосредственных участников – пилотов. Ситуационная осведомленность предполагает наблюдение в реальном времени за всеми ВС с целью определения их идентификаторов, текущих координат (широты, долготы и высоты над уровнем моря), а также направления и скорости движения.

Исторически первым решением проблемы наблюдения воздушного движения явилось использование средств радиолокационного обзора, получившего название первичного радара. Несмотря на ряд серьезных ограничений как по территориальному покрытию, так и по способности идентификации объектов, первичный радар, тем не менее, долгое время использовался как единственное средство наблюдения за воздушным движением.

В настоящее время для цели наблюдения в системе управления воздушным движением (УВД) в основном используются методы вторичной радиолокации (ВРЛ). Локатор сканирует воздушное пространство и измеряет дальность до ВС при известном угловом положении приемо-передающего зеркала локатора. Получив запрос, ВС формирует ответный сигнал, включая в него свой идентификатор, высоту полета и другие параметры. Методы ВРЛ являются достаточно сложными и затратными.

Концепция наблюдения радикально изменилась в конце прошлого столетия после ввода в эксплуатацию группировки навигационных спутников глобального позиционирования GPS. Оснащение всех ВС средствами навигации по сигналам спутников GPS обеспечило значительное повышение точности позиционирования, ликвидировав попутно ее зависимость от удаленности ВС от наземной диспетчерской инфраструктуры. Как следствие, параллельно использованию вторичного радара в настоящее время развивается концепция наблюдения за воздушным движением, получившая название

автоматического зависимого наблюдения радиовещательного типа (АЗН-В).

АЗН-В представляет собой безрадарный метод наблюдения, при котором ВС автономно, например, при помощи средств спутниковой навигации GPS/ГЛОНАСС, определяет свое местоположение и по определенному протоколу, зависящему от выбранной линии передачи данных (ЛПД), сообщает в радиовещательном режиме (то есть всем одновременно, без получения подтверждения сообщения) о своем положении заинтересованным участникам воздушного движения. Международная организация гражданской авиации (ИКАО, ICAO) и авиационные администрации всех ведущих стран первоначально рассматривали АЗН-В как основной метод наблюдения, который должен стать обязательным для гражданской авиации на рубеже 2020 года.

АЗН-В обеспечивает наземное наблюдение воздушных судов без использования радиолокационных станций (РЛС). Может также обеспечиваться ситуационная осведомленность пилотов либо при прямом взаимодействии борт-борт, либо при передаче на борт информации через наземную систему УВД, в том числе о ВС, не оборудованных аппаратурой АЗН-В. Одновременно по мере возможности за счет той же ЛПД стараются обеспечить примыкающие применения (полетно-информационное обслуживание с предоставлением оперативной метеорологической и аэронавигационной информации, навигационное обслуживание в части обеспечения информации о целостности спутниковых навигационных сигналов и дифференциальных поправок, связь пилота по линии передачи данных с диспетчером и/или авиакомпанией, операции по поиску и спасанию и др.).

На начальных этапах технологии АЗН-В развивались по различным направлениям, обусловленным использованием различных ЛПД. В 2003 году на 11-й Аэронавигационной конференции для начального внедрения было рекомендовано использовать АЗН-В на базе ЛПД расширенного сквиттера (extended squitter) на частоте 1090 МГц – 1090 ES (далее – АЗН-В/1090). Тогда же было указано на опасность для такого АЗН-В явления так называемого насыщения/интерференции (наложения сигналов при высокой плотности движения). На той же конференции было указано на необходимость вести работы по другим ЛПД, в частности, по VDL-4 (Very High Frequency Data Link Mode 4). В последующем, благодаря усилиям главным образом FAA и RTCA (США) и EUROCAE (Европа), был разработан целый ряд документов, базирующихся на монопольном использовании АЗН-В/1090 [1, 2].

За время, прошедшее с момента начала разработки систем АЗН-В, в мире произошел целый ряд изменений, поставивших под вопрос целесообразность дальнейшего использования системы 1090 ES в целях АЗН-В:

1. **Критическое повышение плотности воздушного движения**, в том числе за счет развития средств малой авиации, выводящее работу диспетчера в экстренных условиях на грань психофизических возможностей человека.

Система 1090 ES была разработана согласно концепции, игнорирующей мировой опыт и широко принятые правила построения радиотехнических систем. Она предполагает неупорядоченное по отношению друг к другу вещание сигналов различными ВС на одной частоте. Такой принцип функционирования приводит к взаимным помехам при приеме сигналов.

В соответствии с базовыми положениями общей теории связи сигналы различных источников могут быть разделены на приеме только в случае их ортогональности. Ортогональность сигналов может быть обеспечена разделением сигналов либо по частоте (технология частотного разделения каналов FDMA), либо во времени (временного разделения каналов TDMA), либо по форме (CDMA). Эти положения были сформулированы задолго до начала разработки системы 1090 ES, однако они не были учтены разработчиками.

Как-то выполняя функцию поддержки процесса наблюдения в условиях невысокой плотности воздушного трафика, уже в настоящее время система 1090 ES функционирует в условиях потерь до 95% (!) передаваемых сообщений [3, 4]. И какого-либо улучшения перспектив не предвидится.

2. **Взрывное распространение беспилотных летательных аппаратов (БЛА)** различных массогабаритных категорий.

Высокая степень ассортиментной и ценовой доступности БЛА для широких слоев населения в сочетании с отсутствием сегодня единых правил их эксплуатации повышает риск возникновения аварийных ситуаций, вызванных проникновением таких аппаратов в воздушное пространство, отведенное для движения пилотируемых ВС. При массовом характере распространения беспилотников их проникновение в агрегированное воздушное пространство может быть вызвано как ошибками пилотирования, так и техническими сбоями систем управления БЛА. Последнее обстоятельство связано с отсутствием в настоящее

время единых правил, регламентирующих распределение спектрального ресурса между БЛА различных систем и обеспечивающих возможность и безопасность их совместной работы в зоне возможных взаимных электромагнитных влияний. Еще одним фактором риска использования БЛА является возможность потери канала управления летательным аппаратом со стороны станции дистанционного пилота; такая потеря может привести к катастрофическим последствиям.

В [5] была показана непригодность АЗН-В/1090 для наблюдения дистанционно пилотируемых авиационных систем (ДПАС) прежде всего по причине необходимости использования ВРЛ или МПСН на наземных станциях дистанционных пилотов, чего не сможет себе позволить ни одна экономика мира. Кроме того, формат сообщения АЗН-В не обеспечивает достаточной для дополнительного количества БПЛА емкости адресного пространства.

3. **Зависимость системы обеспечения безопасности полетов от инфраструктуры**. Наблюдение за воздушным движением в настоящее время осуществляется, главным образом, двумя видами средств: вторичным радаром и системой сквиттера 1090 ES, сигналы которого принимаются спутниками или специальными наземными средствами с выходом в сеть ATN. Оба вида наблюдения предполагают наличие специализированной инфраструктуры, целесообразность построения которой в конкретной стране в значительной степени определяется геополитическими интересами и реже экономическими – при достаточно высокой плотности населения и уровне развития территорий предполагаемого развертывания.

Геологические и климатические условия во многих странах не обеспечивают экономической эффективности построения соответствующей инфраструктуры, например, зона вечной мерзлоты в северной части России, горный Китай и др. Кроме того, построение наземной инфраструктуры затруднено во многих труднодоступных районах, а также на акватории мирового океана. Так, например, в России многие полеты происходят в так называемом ситуационном режиме, когда пилоты выходят на связь по расписанию, пролетая вблизи крупных городов с развитой авиационной инфраструктурой. В перерывах же между сеансами связи воздушное судно может находиться за пределами системы наблюдения и радиодоступа.

Обязательная привязка ВС к инфраструктуре диспетчерских служб и связанная с ней ограниченность территориального охвата наблюдением наглядно демонстрирует несоответствие действующих систем 1090 ES требованиям времени, о чем свидетельствуют участившиеся в последние годы чрезвычайные происшествия, связанные с исчезновением воздушных судов и их катастрофами по непонятным причинам.

4. **Квалифицированный терроризм**, который может явиться опаснейшим порождением нашего века в авиации. Сохраняя историческую преемственность классического терроризма в стремлении использования все более и более изощренных технических средств и методов, в авиации терроризм получил в 21 веке новые легко доступные и недорогие инструменты уничтожения воздушных судов – БЛА, и средства их наведения на цель – многочисленные радиоконструкторы, выпускаемые различными фирмами с целью демонстрации возможностей выпускаемой элементной базы и ускорения разработок на ее основе. Последний вид инструментария может быть также активно использован для нарушения корректной работы бортовых навигационных и телекоммуникационных систем.

Авиация оказалась неготовой к отражению опасности со стороны квалифицированного терроризма. Внедренная к настоящему времени в большинстве стран мира система АЗН-В/1090 доказала свою беспомощность в новых условиях и полное несоответствие современным требованиям безопасности воздушного движения. Данная система использует для передачи сигналов открытые каналы без каких-либо средств защиты информации. Это очень опасная практика. При известных обстоятельствах система АЗН-В/1090 может стать весомым подспорьем для террористов, открытый характер сообщений которой открывает террористам картину воздушного движения практически по всему миру, поддерживаемую в интернете владельцами сайта Flightradar24.

Квалифицированный терроризм предполагает возможность следующего вида атак:

- радиоперехват с целью определения реальных координат конкретного воздушного суда (по его идентификатору). Обладание одновременно информацией об идентификаторе воздушного суда и его координатах открывает террористу возможность запуска БЛА (возможно, оснащенного взрывным устройством для усиления эффекта), запрограммированного на столкновение с конкретным воздушным судном;

- организация целенаправленных квалифицированных помех, подобных реальным сигналам автоматического зависимого наблюдения-вещания – фантомов. Организация фантомов для террориста – не требующий больших затрат способ заставить ВС (возможно, целенаправленно выбранное) совершить опасный маневр, способный привести к аварии. Например, фантом выезжающего на посадочную полосу снегоуборщика в условиях захода на посадку при ограниченной видимости. Сегодня наиболее простым способом организации фантомов, неотличимых от реально действующих участников воздушного движения, является простая запись в память сигналов автоматического зависимого наблюдения-вещания 1090 ES конкретных ВС и дальнейшее (возможно, многократное) повторное воспроизведение этих сигналов в качестве квалифицированной помехи;
- "завал спамом" экрана диспетчера или ВС. Внезапное появление "из ниоткуда" на дисплее диспетчера множества объектов – фантомов, может заставить его потерять контроль над ситуацией и создать угрозу аварии для всех воздушных судов в районе аэропорта, особенно если ситуационная осведомленность пилотов в окружающем аэропорт воздушном пространстве будет определяться только сообщениями диспетчера;
- атака на сигналы глобальных спутниковых систем навигации. Этот вид атаки подразумевает два вида действий: либо "грубое" подавление спутниковых сигналов наведенной помехой, либо генерацию в эфир сигналов "ложных" спутников, нарушающих адекватную работу системы определения координат приемного оборудования. В любом случае успех атаки может привести к потере ориентации в пространстве воздушного суда или группы воздушных судов, а для БЛА – нарушить работу системы управления, создавая опасность столкновения с пилотируемыми ВС;
- геополитический терроризм. Использование на территории страны стандарта 1090 ES ставит воздушное движение в зависимость от поведения другой страны, что не представляется допустимым для суверенного государства.

Проведенный анализ дает основание расставить акценты в вопросах выбора направлений решения проблемы безопасности полетов в воздушном пространстве страны. Необходимость обеспечения пилотов информацией о наличии и координатах в окружающем пространстве ВС и других объектов (например, спецтехники на взлетной или посадочной полосах) в автоматическом или автоматизированном режимах требует разработки новых средств повышения степени безопасности воздушного маневрирования и снижения нагрузки на диспетчеров. Эти цели могут быть достигнуты в рамках альтернативной системы VDL-4, например, за счет использования сетевых технологий.

Интересы безопасности полетов диктуют необходимость разработки концепции и средств обеспечения информационной безопасности системы АЗН-В, гарантирующих защиту от:

- перехвата сообщений, содержащих одновременно идентификатор ВС и его координаты, несанкционированными органами или частными лицами;
- навязывания ложной информации со стороны террористов и легальных участников воздушного движения;
- возможности отрицания легальным участником воздушного движения фактов передачи в эфир сообщений АЗН-В;
- повторов ранее переданных сообщений, дублируемых "в записи" террористами или легальными участниками воздушного движения;
- возможности навязывания террористами или легальными участниками движения сообщений "от чужого имени" – от лица других участников движения;
- подавления или/и выдачи ложных сигналов глобальных спутниковых систем навигации.

Решение задачи защиты осложняется двумя противоречивыми требованиями.

С одной стороны, передаваемая информация должна быть надежно защищена от всех посторонних лиц, среди которых могут оказаться террористы.

С другой стороны, она должна быть открыта для доступа диспетчерам и пилотам всех ВС всех стран как средство предупреждения столкновений.

Задача обеспечения информационной безопасности в представленной постановке не может быть решена в рамках использования системы АЗН-В на базе 1090 ES.

Большая группа специалистов из США в течение более 15 лет постоянно работает над улучшением

стандарта для АЗН-В/1090. Количество модификаций стандарта – DO-260, DO-260A, DO-260B, DO-260C – уже измеряется двузначной цифрой. После одной из таких модификаций аппаратуру АЗН-В/1090 пришлось заменить на доработанную по новому стандарту на тысячах ВС гражданской авиации США, находящихся в эксплуатации. Работа над очередной новой модификацией стандарта DO-260B идет полным ходом.

Проблема информационной безопасности не исчерпывается обеспечением конфиденциальности, а включает также следующие составляющие:

- аутентификацию источника сообщений и связанную с ней неотрекаемость авторства источником сообщения;
- идентификацию целостности сообщений;
- контроль доступа, включающий защиту от повторов "в записи" ранее переданных сообщений.

За последние полтора десятилетия в разных странах предпринимались активные, но безуспешные попытки решить задачу обеспечения информационной безопасности системы АЗН-В/1090 различными средствами, включая криптографию и, в частности, формат DF-19. Анализ результатов проведенных работ, выполненный по 118 литературным источникам, изложен в [6]. Его главный результат – вывод о невозможности обеспечения требуемого уровня информационной защиты в рамках системы АЗН-В/1090.

Итогом работ по криптографической защите сообщений АЗН-В явилась разработка криптографического алгоритма FFX, представленного на утверждение в NIST еще в 2010 году. Сведений о его утверждении на уровне Approved к настоящему моменту не имеется.

Алгоритм FFX строится на базе машины Фейстеля (сети Фейстеля) с использованием оригинальных мер для усечения шифруемого сообщения до нестандартных размеров более сильными криптографическими алгоритмами. Предлагаемый размер шифруемого блока составляет 104 бита и соответствует части 112-битного сообщения системы АЗН-В/1090.

К настоящему времени интерес к алгоритму FFX заметно иссяк вследствие низкой перспективной эффективности его использования в широких масштабах.

Главная проблема использования алгоритма FFX в приложении АЗН-В/1090 заключается в том, что в состав шифруемой части сообщения включен идентификатор ВС, что по умолчанию предполагает использование одного общего ключа для всех участников воздушного движения.

Использование единого ключа для всех участников информационного обмена не представляется эффективной мерой ввиду невозможности его надежного хранения, вследствие чего главные задачи шифрования – обеспечение конфиденциальности сообщений и аутентификации – не решаются. Шифрование более короткого участка сообщения АЗН-В/1090 (52 бита) не обеспечит необходимой степени криптостойкости.

Наиболее адекватным средством решения задачи обеспечения информационной безопасности в сложившихся условиях представляется использование двухключевых (Public Key) алгоритмов криптографической защиты информации. Эти алгоритмы, обеспечивая необходимые функции, требуют в рамках поставленной задачи использования обмена информацией между объектами в диалоговом режиме.

Главной причиной невозможности обеспечения представленных функций и требуемого уровня информационной защиты в рамках системы АЗН-В/1090 является отсутствие протоколов диалогового обмена в ее составе.

Использование этих алгоритмов предполагает наличие открытого ключа, находящегося в постоянном распоряжении криптоаналитика – террориста. Обладая открытым ключом и определенным запасом времени, криптоаналитик может создать некоторый "словарь" основных зашифрованных сообщений известного содержания и распознавать эти сообщения в передаваемых в эфир сигналах АЗН-В.

Внесение временных меток (каждый раз новой) в состав шифруемых сообщений лишает смысла процесс составления "словаря", повышая степень информационной безопасности канала связи. Наличие временных меток обеспечивает возможность защиты от повторов ранее переданных сообщений, записанных криптоаналитиком. Эта проблема актуальна при использовании как одноключевых, так и двухключевых криптографических алгоритмов, например, от "завала спамом" дисплея пилота или диспетчера.

Необходимый уровень безопасности полета в текущих условиях можно обеспечить за счет внедрения системы информационной безопасности в соответствии со следующими требованиями:

- система должна быть снабжена автоматическими невыключаемыми/неостанавливаемыми средствами наблюдения, сигнал от которых, несущий идентификатор ВС, временные и пространственные координаты, должен быть защищен криптографическими

средствами от перехвата террористами и несанкционированными пользователями;
- процесс наблюдения должен быть защищен от неверной информации, поступившей из несанкционированных источников; источники всех сообщений должны быть аутентифицированы и проверены на подлинность; прием информации из несанкционированных источников должен стать невозможным. Получатель сообщения должен иметь возможность убедиться, что принятое сообщение не было изменено при передаче; у нарушителя не должно быть возможности заменить подлинное сообщение на ложное. Получатель должен иметь возможность убедиться в его происхождении; нарушитель не должен иметь возможности замаскироваться под кого-либо другого;
- система должна предоставить поддержку функции идентификации, обеспечивая возможность отличать фантомы от реальных ВС;
- система должна позволить определить местонахождение сигналов-призраков, чтобы надлежащим образом подавить их;
- должна быть обеспечена неотрекаемость: у отправителя не должно быть возможности ложно отрицать позднее факт посылки сообщения. Кроме того, получение каждого сообщения сопровождается подтверждением и пересылкой отправителю уведомления об этом, включая регистрацию у получателя;
- необходимо обеспечить в масштабе системы возможность управления и навигации ВС на случай подавления сигналов GNSS;
- в целях записи и последующей интерпретации событий, включая поисково-спасательные работы, сигналы АЗН-В следует соотнести со шкалой времени (метка времени); это позволит записать положение всех ВС в 4-х измерениях. Метки времени в системе безопасности исключат дублирование ранее записанных сообщений;
- все действия по обеспечению безопасности должны строиться на основном принципе, когда применяемые меры должны быть соизмеримыми с угрозами. После оценки риска, проводимой соответствующими национальными полномочными органами, должна быть обеспечена разработка мер защиты критически важных систем информационных и связных технологий, используемых для целей гражданской авиации, вмешательство в которое может поставить под угрозу безопасность полетов. Политика риска должна быть прозрачной, предсказуемой и контролируемой, сосредоточенной на самом высоком риске, объективной. Должны применяться разработка степеней безопасности и соответствующая стандарту ARP 4754A SAE классификация условий отказов. Для всех классов условий отказа (типа катастрофических, опасных/жестких крупных, крупных, мелких и отсутствия влияния на безопасность) соответствующие вероятности должны назначаться единым для всех высокоинтегрированных бортовых систем образом;
- помимо защиты от несанкционированного доступа и использования, система безопасности должна обнаруживать кибератаки, обеспечивая надлежащую защиту от вирусов и хакерских программ, выполняя записи, анализ и разработку соответствующего противодействия;
- криптографические алгоритмы, используемые в системе, должны иметь подтвержденный статус (Approved), средства защиты должны быть сертифицированы. Длина ключа должна обеспечивать требуемый уровень защиты. При использовании двухключевых алгоритмов криптозащиты система должна обеспечивать устойчивость к попыткам составления террористом "словаря" зашифрованных открытым ключом алгоритма сообщений известного содержания, дающего возможность распознавания их в составе потока сообщений.

Реализация представленных выше требований может базироваться на протоколах, поддерживающих диалоговый характер обмена информацией. Результаты зарубежных исследований, объединившие 118 литературных источников [6], показали невозможность обеспечения требуемого уровня информационной защиты в рамках системы АЗН-В/1090. Криптографические средства 1090 ES и, в частности, формат DF-19 не обеспечивают защиту от спуфинга, поскольку используют единый ключ для всех участников информационного обмена. Размер информационных блоков не согласован с алгоритмами шифрования, криптостойкость которых аттестуется как Approved по требованиям NIST. И, самое главное, система АЗН-В/1090 не поддерживает диалоговых протоколов обмена информацией, что является препятствием к использованию двухключевых

криптографических алгоритмов и формированию сеансовых ключей.

Решение поставленных проблем может быть достигнуто использованием самоорганизующихся сетевых технологий – построением А-сети на основе специальных коммутирующих радиотранспондеров, функционирующих на базе протоколов VDL-4. Как система автоматического зависимого наблюдения-вещания, А-сеть является альтернативой системе стандарта 1090 ES, исключающей использование результатов наблюдений другими странами в разведывательных целях и снимающей зависимость процесса наблюдения от действий другой страны. Системный подход к процессу наблюдения за воздушными судами в рамках А-сети снимет проблему наложения во времени сигналов разных воздушных судов, передаваемых на одной частоте, и обусловленные этим положением взаимные помехи.

Защита информации в А-сети строится на основе двухключевых алгоритмов криптозащиты в режиме обмена точка-точка и для формирования группового сеансового ключа для использования симметричных криптографических алгоритмов в вещательном режиме для группы объектов.

Каждому сетевому объекту должна быть присвоена пара ключей – один открытый и один закрытый. Все открытые ключи хранятся в общей базе данных, доступной только уполномоченному персоналу, включая дежурных пилотов. Закрытые ключи физически защищены, будучи встроены в оборудование без логического доступа вне функции шифрования/дешифрования.

Каждое ВС оснащается двухключевой криптосистемой. Каждое передаваемое в режиме точка-точка сообщение шифруется открытым ключом адресата и аутентифицируется закрытым ключом источника, любая пара сетевых объектов должна использовать алгоритмы с открытым ключом для защиты и аутентификации взаимного трафика.

Этот механизм эффективен для связи между парой объектов, однако он исключает вещательный режим и приводит к значительному непроизводительному увеличению трафика для обмена информацией между группой объектов. Для решения этой проблемы следует использовать комбинированное применение симметричных криптографических алгоритмов и алгоритмов с открытым ключом. Защита вещательного режима должна быть организована на основе симметричного криптографического алгоритма, а алгоритм шифрования с открытым ключом должен использоваться для обмена групповыми ключами или для генерации сеансовых ключей.

На сегодня одним из лучших решений, удовлетворяющих сформулированным требованиям, является использование шифрования на основе эллиптических кривых. Криптостойкость асимметричной системы, в частности системы на эллиптических кривых, строится на сложности решения задачи дискретного логарифмирования. Сложность решения, а значит и время выполнения, напрямую зависят от размера (битовой длины) сообщения/ключа.

В системе АЗН-В/VDL-4 длина сообщения ограничена 160 битами. Если злоумышленник будет использовать ро-алгоритм Полларда, имеющего сложность $O(\sqrt{((\pi \cdot p)/2)})$, то на вычисление закрытого ключа по открытому даже на самом мощном суперкомпьютере в мире Summit потребуется чуть более 175 дней. За это время информация потеряет свою актуальность.

Синхронный характер сети обеспечивает возможность использования мультилатерационных механизмов – как для локализации источников злонамеренных воздействий, так и в целях навигации в отсутствие сигналов ГНСС.

ЛИТЕРАТУРА

1. Minimum Aviation System Performance Standards for Aircraft Surveillance Applications (ASA), Vol. 1–2. – RTCA, DO-289, 2003.
2. Минимальные требования стандартов к характеристикам авиационных систем – автоматическое зависимое наблюдение в радиовещательном режиме (АЗН-В). – RTCA, DO-242A, 2005.
3. RTCA DO-260C-draft Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B). – RTCA.
4. **Мирошниченко А.В., Татарчук И.А., Фальков Э.Я., Шаврин С.С.** Сравнение пропускной способности систем автоматического зависимого наблюдения – вещания // ПЕРВАЯ МИЛЯ. 2020. № 3. С. 24–29.
5. **Фальков Э.Я.** Интеграция беспилотных авиационных систем в общее воздушное пространство: ключевые проблемы и возможные пути решения // Крылья Родины. 2016. № 2. С. 25–31.
6. **Strohmeier M., Lenders V., Martinovic I.** On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. ArXiv:1307.3664v2 [cs.CR] 15 Apr. 2014.

МФЭС

РОССЕТИ

МЕЖДУНАРОДНЫЙ ФОРУМ «ЭЛЕКТРИЧЕСКИЕ СЕТИ»

1-4 ДЕКАБРЯ 2020

Москва, ВДНХ, 75 павильон

При поддержке

РОССЕТИ

Организатор

ЗАО «ЭЛЕКТРИЧЕСКИЕ СЕТИ»

Оператор

Grata adv

expoelectroseti.ru

vk.com/electrosetiforum

facebook.com/forumelectroseti

instagram.com/expoelectroseti