УДК 629.7.058:351.814.3
DOI: 10.26467/2079-0619-2019-22-1-39-50

ОБЗОР ОСНОВНЫХ ПУТЕЙ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ АЗН-В

В.В. КОСЬЯНЧУК[1], Н.И. СЕЛЬВЕСЮК[1], Р.Р. ХАММАТОВ[1]
[1]Федеральное государственное унитарное предприятие «Государственный научно-исследовательский институт авиационных систем», г. Москва, Россия

Работа выполнена при финансовой поддержке РФФИ, гранты № 18-08-463, № 18-08-453

Автоматическое зависимое наблюдение радиовещательного типа (АЗН-В) является важным средством обеспечения безопасности и эффективности воздушного движения. В перспективе роль АЗН-В будет увеличиваться. В то же время киберзащищенность АЗН-В является явно недостаточной. В статье анализируется проблема низкой защищенности АЗН-В. Основными причинами уязвимости АЗН-В являются открытость системы и современные достижения в развитии компьютерных технологий и программируемого радио. Приводится классификация вероятных атак на систему АЗН-В с определением целей, сложности реализации и ущерба от проведения атаки. Сделан вывод, что аналогичными уязвимостями обладают и другие авиационные радиотехнические системы и требуется комплексное решение проблемы повышения уровня безопасности. Основными причинами недостаточной безопасности авиационных систем связи, навигации и наблюдения являются: долговременность циклов разработки и сертификации, требования унаследованности и совместимости, ценовое давление, перегрузка частот и предпочтение открытых систем. В работе сделан обзор основных путей повышения безопасности системы АЗН-В. Показано, что все методы повышения безопасности можно разделить на две группы: методы, основанные на идентификации и аутентификации абонентов вещательных радиосетей, и методы, основанные на верификации данных, передаваемых по вещательным радиосетям неаутентифицированными абонентами. Методы первой группы реализуют алгоритмы типа «идентификация-аутентификация» и могут быть разделены на некриптографические и криптографические, последние могут использовать симметричное либо асимметричное шифрование. Методы второй группы основаны на различных алгоритмах верификации данных от системы АЗН-В с некоторыми дополнительными данными, полученными по другим каналам или от иных источников. Рассмотрены методы второй группы: мультилатерация, ограничение расстояния, калмановская фильтрация, статистическая проверка гипотез, групповая верификация, проверка на правдоподобие и использование дополнительных данных. В статье приводятся примеры использования некоторых методов повышения безопасности системы АЗН-В, их достоинства и недостатки.

Ключевые слова: атака, безопасность, верификация, идентификация, киберзащищенность, наблюдение, уязвимость, АЗН-В.

ВВЕДЕНИЕ

Объемы воздушных перевозок с каждым годом неизменно увеличиваются. Стремление к уменьшению воздействия авиации на окружающую среду и более эффективному использованию воздушного пространства и воздушных судов (ВС) обусловливает требование повышения эксплуатационной гибкости при неизменном или более высоком уровне безопасности. Безопасная организация все более масштабного и сложного воздушного движения требует применения более совершенных инструментов и средств. Одним из таких важных инструментов в процессе организации воздушного движения (ОрВД) является авиационное наблюдение, в частности автоматическое зависимое наблюдение радиовещательного типа (АЗН-В)[1].

В системе АЗН-В осуществляется радиовещательная передача с борта воздушного судна данных о его местоположении (координаты: широта, долгота), абсолютной высоты, скорости, опознавательного индекса, качества навигационных данных и другой информации, полученной от бортовых систем. Данные о местоположении и скорости ВС, как правило, получают от бор-

[1] Aeronautical Surveillance Manual. Doc 9924 AN/474. 2nd ed. ICAO. Montreal, 2017.

товой глобальной навигационной спутниковой системы (GNSS). Показатели качества навигационных данных определяются при помощи спутниковой системы функционального дополнения SBAS[2]. Сообщения АЗН-В передаются в радиовещательном режиме, и их может получать и обрабатывать любой подходящий приемник. Структура АЗН-В представлена на рис. 1.

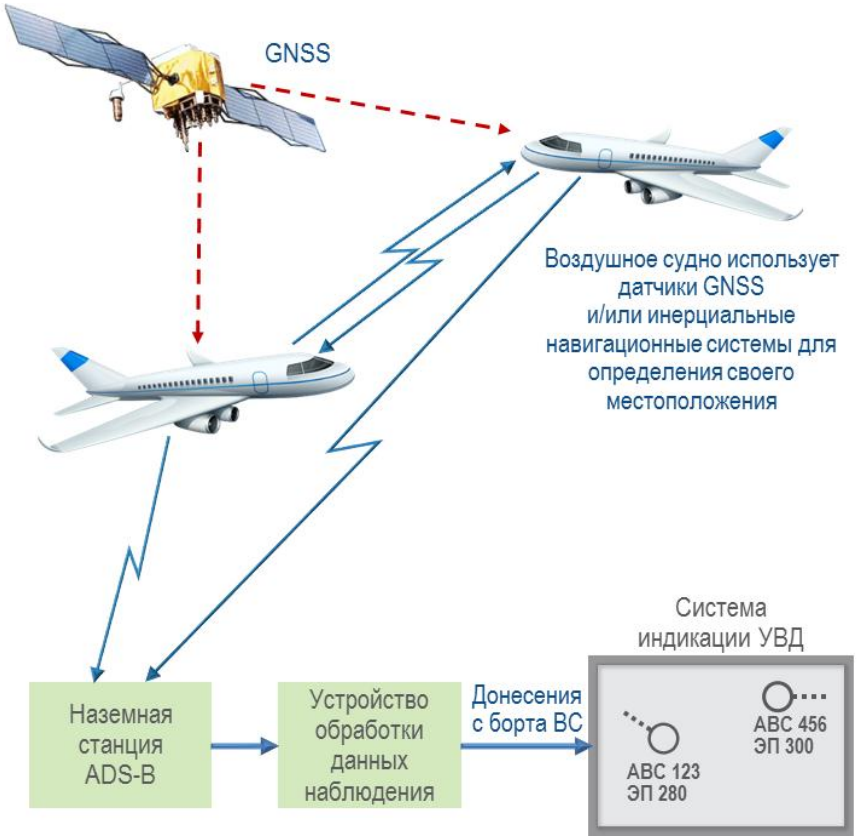

Рис. 1. Система АЗН-В
Fig. 1. ADS-B system

Сегодня АЗН-В рассматривается Международной организацией гражданской авиации (ICAO) в качестве основного метода наблюдения. Совместное наблюдение на основе имеющихся в настоящее время технических средств с использованием полос радиочастот 1030/1090 МГц (SSR, режима S, WAM и ADS-B) является важной тенденцией в течение ближайших десятилетий[3]. Авиационные администрации США и Европы заявляют в программах NextGen[4] и SESAR[5] соответственно об обязательном оснащении воздушных судов системой АЗН-В. В Российской Федерации также проводятся мероприятия по широчайшему внедрению АЗН-В[6,7]. Таким образом, следует ожидать, что в ближайшее время АЗН-В будет повсеместно

[2] Aeronautical Telecommunications. Vol. I. Radio Navigation Aids. 6th ed. / Annex 10 to the Convention on International Civil Aviation. ICAO. Montreal, 2006.
[3] 2016–2030 Global Air Navigation Plan. Doc 9750 AN/963.5thed. ICAO. Montreal, 2016.
[4] Concept of Operations for the Next Generation Air Transportation System / Joint Planning and Development Office. Washington, 2007.
[5] European ATM Master Plan: The Roadmap for delivering high-performing aviation in Europe. Executive View / SESAR. 2015 ed.
[6] Поддержание, развитие и использование системы ГЛОНАСС (2012–2020 годы): федеральная целевая программа: утв. постановлением Правительства Российской Федерации от 3 марта 2012 года № 189.
[7] Концепция внедрения автоматического зависимого наблюдения на основе единого стандарта с развитием до функционала многопозиционных систем наблюдения в Российской Федерации: утв. распоряжением Минтранса России от 25 апреля 2018 года № 68.

внедряться, использоваться, усовершенствоваться и модернизироваться, т. е. в целом играть одну из ключевых ролей в наблюдении.

Вместе с тем в АЗН-В отсутствуют явные механизмы для защиты конфиденциальности, целостности и доступности данных, передаваемых между воздушными судами и авиадиспетчерами, что делает такую систему уязвимой для угроз кибертеррористического характера, особенно актуальных в связи с современным развитием компьютерных технологий и программируемого радио (SDR – Software Defined Radio). Этой актуальной проблеме посвящена настоящая статья, в ней рассматриваются методы, которые могли бы повысить безопасность системы АЗН-В.

ПРОБЛЕМА НИЗКОЙ ЗАЩИЩЕННОСТИ АЗН-В

Проблема низкой защищенности АЗН-В не является новой и достаточно широко освещена в технической и научно-популярной литературе [1–10]. В настоящей статье главное внимание будет уделено системе АЗН-В, базирующейся на использовании ЛПД с 1090-МГц расширенным сквиттером (АЗН-В 1090 ES), так как именно эта ЛПД принята на сегодняшний день в качестве основной для создания единой системы на государственном и международном уровнях[8,9,10].

Среди основных причин незащищенности АЗН-В можно особо выделить две:

– система изначально разрабатывалась в предположении, что каждый участник должен иметь возможность наблюдать всех остальных, т. е. система открыта для любого участника;

– на момент разработки системы серьезных кибертеррористических угроз не существовало, или они были маловероятны, или ошибочно считалось, что они маловероятны.

В результате система АЗН-В легко подвержена спуфингу и другим видам атак. В значительной степени это связано с широким распространением таких дешевых и мощных устройств, как средства радиосвязи с программируемыми параметрами (SDR).

Рассмотрим классификацию атак, которые могут угрожать АЗН-В. Основные виды атак будут приведены в соответствии с классификацией атак, изложенной в [3].

- ***Рекогносцировка воздушного судна.*** Характеризуется попыткой извлечения информации о движении воздушного судна. Эта атака может также являться подготовительным этапом к более сложной атаке.
- ***Прямое подавление наземной станции.*** Блокировка передачи на частоте 1090 МГц с использованием постановщика помех. Характеризуется отсутствием прицельности, т. е. действует на все объекты в зоне подавления, ограниченной техническими характеристиками передатчика помех.
- ***Вброс ложной цели на наземной станции.*** Формирование и передача в эфир фальшивых сообщений, которые приводят к появлению на пульте диспетчера ложной отметки.
- ***Прямое подавление бортовой станции.*** То же, что и прямое подавление наземной станции, только целью атаки является воздушное судно. Целевое воздушное судно должно быть оснащено оборудованием АЗН-В In.
- ***Вброс ложной цели на бортовой станции.*** То же, что и вброс ложной цели на наземной станции, только целью атаки является воздушное судно. Целевое воздушное

[8] Concept of Operations for the Next Generation Air Transportation System / Joint Planning and Development Office. Washington, 2007.

[9] European ATM Master Plan: The Roadmap for delivering high-performing aviation in Europe. Executive View / SESAR. 2015 ed.

[10] Концепция внедрения автоматического зависимого наблюдения на основе единого стандарта с развитием до функционала многопозиционных систем наблюдения в Российской Федерации: утв. распоряжением Минтранса России от 25 апреля 2018 года № 68.

судно должно быть оснащено оборудованием АЗН-В In. Воздействие атаки аналогично воздействию атаки прямого подавления воздушного судна.

- ***Комбинации одного или нескольких обозначенных выше типов.***

Представленная классификация показывает, что целями атаки могут являться воздушное судно (воздушные суда) либо наземная станция (диспетчер); методами атаки могут быть перехват, прямое подавление или излучение ложных сигналов. Трудность таких атак характеризуется в [3] от низкой до средне-высокой. Наиболее сложно реализуемой атакой является нацеливание на наземную станцию для вброса сообщений. Вредное воздействие от атак может проявляться в виде утраты конфиденциальности, снижения доверия к системе, потери управления.

Необходимо отметить, что проблема незащищенности или недостаточной защищенности присуща не только АЗН-В, но и множеству других не менее важных радиотехнических авиационных систем, например GNSS, голосовая и цифровая ОВЧ-связь (VHF, CPDLC, ACARS), информационные службы (TIS-B, FIS-B), системы наблюдения и предупреждения столкновения (PSR, SSR, MLAT, TCAS) и т. д. При этом становится очевидной необходимость комплексного решения проблемы кибербезопасности для всего спектра средств связи, навигации и наблюдения. В противном случае, при всесторонней защите только системы АЗН-В, остается возможность проведения атак на другие системы – GNSS или голосовой связи. Организовать постановку помех для этих систем не намного сложнее, чем поставить помеху АЗН-В, а результат будет примерно одинаков, а возможно и хуже. В такой ситуации только комплексный подход к решению задачи обеспечения кибербезопасности воздушного судна (авиационной системы, авиационного комплекса) позволит получить эффективный, надежный и безопасный результат.

Возвращаясь к причинам уязвимости столь обширной группы систем авиационной электросвязи, можно кратко указать следующие [4, 5].

- ***Длительные циклы разработки и сертификации.*** Циклы разработки и внедрения новых технологий в авиации доходят до двадцати и более лет. Такая длительность объясняется большим количеством испытаний и сертификаций для достижения «безопасного уровня» технологии. При этом часто не учитывается возросший вредоносный потенциал и изменение модели угроз, вызванное усовершенствованиями в беспроводных технологиях.
- ***Требования унаследованности и совместимости.*** В гражданской авиации сохраняются старые технологии не только в качестве резерва и по причинам капиталовложений, но также благодаря наибольшей возможной совместимости для управления воздушным движением во всем мире.
- ***Ценовое давление.*** Авиационная отрасль имеет конкурентный характер и находится под значительным ценовым давлением. Изменения для оснащения существующих воздушных судов обходятся дорого и поэтому непопулярны, если только они не обеспечивают незамедлительные финансовые или технологические выгоды эксплуатантам воздушных судов, которые оплачивают расходы на внедрение новых технологий.
- ***Перегрузка частот.*** Некоторые частоты УВД, в частности 1090-МГц канал, сильно загружены. Количество воздушных судов все возрастает, при этом они одновременно используют одни и те же частоты. Ситуация усугубляется еще и увеличением количества полетов беспилотных ВС (БВС), которым будет разрешено входить в контролируемое воздушное пространство в обозримом будущем.
- ***Предпочтение открытых систем.*** Протоколы связи воздушного движения открыты для каждого пользователя. Несмотря на существующие проблемы защиты и конфиденциальности, в ICAO планируется создание будущих протоколов с открытым доступом. Предполагается, что такой подход позволит выполнить такие типичные авиационные требования, как простота связи, совместимость и борьба с административными различиями между странами и классами воздушного пространства.

ОБЗОР ОСНОВНЫХ ПУТЕЙ РЕШЕНИЯ ПРОБЛЕМЫ

Все методы защиты вещательных радиосистем можно разделить на две большие группы. К первой группе относятся методы, основанные на идентификации и аутентификации абонентов вещательных радиосетей. Ко второй группе относятся методы, основанные на верификации данных, передаваемых по вещательным радиосетям неаутентифицированными абонентами. Кроме того, методы защиты можно разделять на позволяющие обнаруживать атаку либо на позволяющие обнаруживать и предотвращать атаку.

Методы первой группы реализуют алгоритмы типа «идентификация-аутентификация» и могут быть разделены на некриптографические и криптографические, последние могут использовать симметричное либо асимметричное шифрование.

Некриптографические схемы включают различные методы для аутентификации пользователей и идентификации радиостанций на основе аппаратных или программных несовершенств или характеристик беспроводного канала, которые трудно копировать. Цель таких схем – установление подозрительных действий в сети. Такие методы в настоящее время вряд ли могут быть с успехом применены в гражданской авиации, но находят применение, например, в задачах государственного опознавания.

Аутентификация сообщений в вещательных средствах сложнее, чем в двухточечных линиях связи. Свойство симметрии полезно только для двухточечной аутентификации, когда два участника доверяют друг другу. Здесь возникает немало трудностей, связанных с генерированием, хранением, управлением, распределением и уничтожением ключей. Таким образом, по существу, требуется асимметричный механизм, чтобы приемники могли верифицировать сообщения, но не имели возможности самостоятельно генерировать аутентичные сообщения.

Здесь следует обозначить целый пласт решений, основанный на использовании ЛПД с методом доступа TDMA (например, VDL режима 4) [6, 7, 11, 12]. Например, предлагается использовать асимметричное шифрование на канальном уровне с использованием открытого и закрытого ключей. Схема подобного решения проиллюстрирована на рис. 2. Для того чтобы существовала возможность отправки сообщений нескольким адресатам (вещательный режим), формируется общий сессионный ключ. Каждое вещательное сообщение подписывается отправителем и шифруется общим сессионным ключом. Получатели дешифруют сообщения сессионным ключом и открытым ключом отправителя. Таким образом, использование шифрования передаваемых данных позволяет обеспечить необходимый уровень защиты. На сегодняшний день ЛПД VDL режима 4 не используется большинством государств для целей АЗН-В, поэтому такое решение не может являться приемлемым в смысле глобального применения в ближайшей перспективе.

Методы второй группы предполагают использование различных алгоритмов верификации данных от системы АЗН-В с некоторыми дополнительными данными, полученными по другим каналам или от иных систем. При этом, как правило, должно быть выполнено отождествление двух или более местоположений или каких-либо отдельных параметров местоположения. Верификация является весьма полезным средством для повышения защищенности АЗН-В. В обновленной второй редакции Руководства по аэронавигационному наблюдению[11] имеется непосредственное указание на необходимость в целях снижения уязвимости от спуфинга сопоставления данных АЗН-В с другими данными, такими как данные полета, профили полета в системе обработки полетных данных и результаты наблюдения от других источников, таких как радар и мультилатерация, если таковые имеются.

[11] Aeronautical Surveillance Manual. Doc 9924 AN/474. 2nd ed. ICAO. Montreal, 2017.

Рис. 2. Процесс обмена зашифрованными сообщениями (из [8])
Fig. 2. Encrypted message exchange process (from [8])

Верификацию местоположения можно выполнять различными способами [13, 14]. Рассмотрим основные способы верификации, которые могут быть использованы для повышения безопасности системы АЗН-В.

- ***Мультилатерация (MLAT).*** Система мультилатерации представляет собой, по сути, разностно-дальномерную радионавигационную систему и является формой независимого кооперативного наблюдения. Таким образом, определение местоположения базируется на вычислении разностей моментов времени прихода сигнала на несколько разнесенных в пространстве приемников. Поверхностями положения являются гиперболоиды, отчего данная система также называется гиперболической (так же, как и радиотехническая система дальней навигации типа LORAN, РСДН). Основной принцип функционирования системы мультилатерации проиллюстрирован на рис. 3.
  Мультилатерация является предпочтительным решением для верификации местоположения наземными средствами или службами. Она используется в США, в Европе и в РФ. Важным преимуществом мультилатерации служит то, что она может использовать уже имеющиеся средства связи воздушного судна. Таким образом, не требуются изменения существующей в настоящее время инфраструктуры воздушного судна, но должны использоваться наземные приемные станции и центральные станции обработки.
  В настоящее время активно проводятся исследования по широкозонной мультилатерации. В сравнении с первичными РЛС широкозонная мультилатерация относительно проста и экономически эффективна для реализации и использования на земле.
  Системы мультилатерации несвободны от недостатков, основными среди которых являются: восприимчивость к многолучевому распространению, необходимость правильного обнаружения сигнала на относительно большом числе приемных станций, требование отдельной линии связи между центральной станцией обработки и приемниками.
  Сложность проведения атак на MLAT относительно высока, особенно если сравнивать со спуфингом контента незащищенных протоколов УВД.

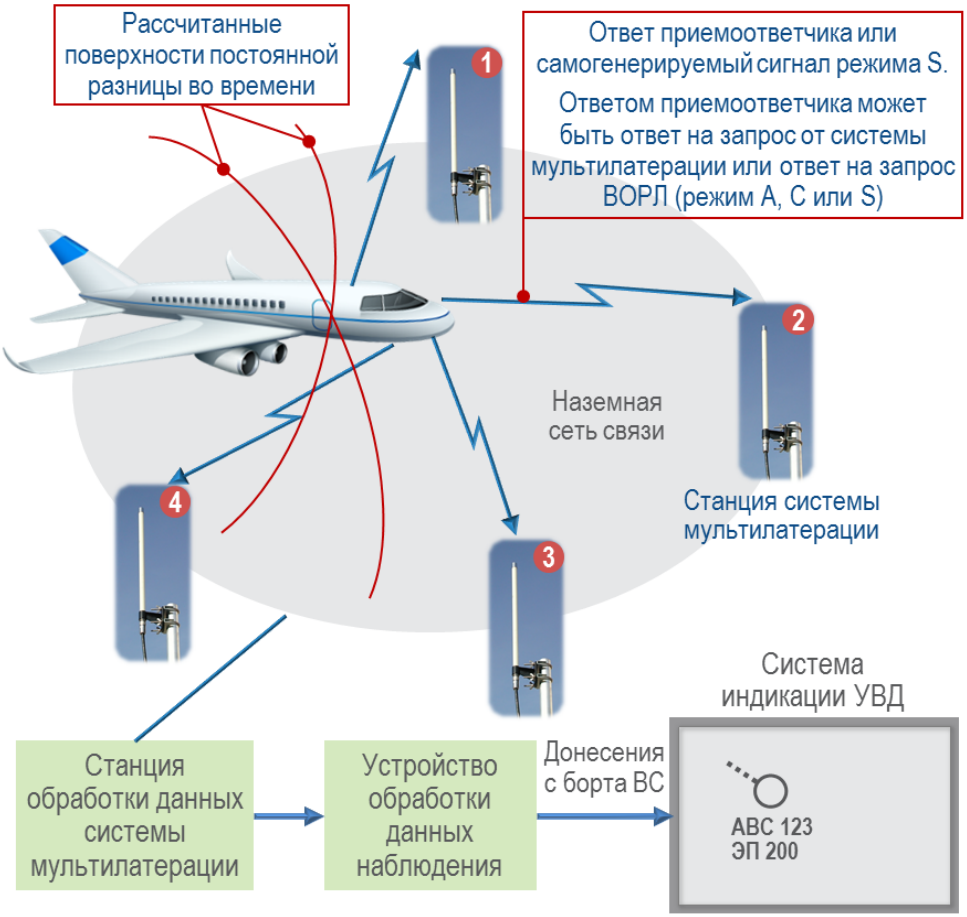

Рис. 3. Система мультилатерации
Fig. 3. Multilateration system

- ***Ограничение расстояния.*** Идея ограничения расстояния заключается в установлении криптографического протокола для наличия подтверждающего абонента, показывающего проверяющему абоненту, что подтверждающий абонент находится в пределах определенного физического расстояния. Это позволяет рассчитать расстояние на основе времени распространения радиосигнала между запросом проверяющего и соответствующим ответом подтверждающего.
  В авиации определенное расстояние может служить верхней границей, дополнительной частью информации, которая может впоследствии использоваться в качестве средства верификации и аутентификации воздушного судна путем проверки истинности заявлений. Метод ограничения расстояния различными доверенными объектами (например, наземными станциями) может использоваться совместно с MLAT для обнаружения действительного местоположения подтверждающего ВС. Кроме того, при учете разностей в уровне принимаемого сигнала можно уменьшать атаки на основе увеличения расстояния и базовые атаки на протокол. Это демонстрирует возможность объединения различных методов физического уровня для повышения теоретической защиты. Однако трудно решить практические проблемы при использовании таких протоколов в УВД.
- ***Калмановская фильтрация.*** Методы калмановской фильтрации находят широкое применение в задачах верификации. Обыкновенно фильтр Калмана работает итерационно в режиме «предсказание» – «коррекция», при этом оперирует не только оценка-

ми вектора состояния, но еще и оценками неопределенности вектора состояния (корреляционная матрица ошибок фильтрации).

На этапе предсказания фильтр Калмана экстраполирует значения переменных состояния, а также их неопределенности. На втором этапе должны быть обработаны данные измерения и результат экстраполяции уточняется. Таким образом, в любой момент времени имеется оценка вектора состояния и оценка корреляционной матрицы ошибок фильтрации (экстраполированные либо уточненные по результатам измерений). Данные оценки могут быть использованы для верификации поступающих данных, например методом отождествления по критерию χ^2.

Калмановская фильтрация позволяет обнаруживать фиктивные маневры, скорости, дальности или другие признаки и значительно повышает сложность атак.

- ***Статистическая проверка гипотез.*** Для решения задачи верификации можно использовать методы статистической проверки гипотез. В этом случае выстраивается линейка гипотез относительно намерений по изменению местоположения каждого наблюдаемого объекта. Вновь полученные данные используются для проверки гипотез, наиболее правдоподобные из которых принимаются за истинные.

  Данные, которые не удовлетворяют ни одной из гипотез, считаются подозрительными. Подозрительные данные могут являться либо реальными незлонамеренными объектами, только что появившимися в поле зрения, либо ложными данными, являющимися атакой на систему. Далее процесс повторяется.

  Таким образом начинают «вязаться» траектории всех наблюдаемых истинных объектов. В процессе обработки последующих наблюдений несогласованные данные могут быть исключены. Применение статистической проверки гипотез усложняет проведение атак, особенно если этот метод используется в совокупности с другими методами, например MLAT.
- ***Групповая верификация.*** Групповая верификация – это мультилатерация, выполняемая группой воздушных судов. Для выполнения такой мультилатерации необходима группа, состоящая из четырех или более находящихся во взаимной радиовидимости воздушных судов. Каждый член группы должен быть уверен в том, что остальные члены группы – реальные незлонамеренные воздушные суда. В большинстве случаев для установления взаимного доверия потребуется аутентификация.

  Мультилатерация выполняется посредством взаимного радиообмена разностно-дальномерным способом или методом учета разностей в уровне принимаемого сигнала. В результате выполнения мультилатерации каждое не входящее в группу воздушное судно будет отнесено либо к «фальшивому», либо к доверенному. В последнем случае такое воздушное судно должно быть включено в группу.

  Групповая верификация существенно увеличивает сложность выполнения атак, хотя и обладает рядом недостатков. Основные недостатки – необходимость организации новых протоколов и помехозащищенных каналов связи, необходимость выполнения аутентификации, сложность процедуры включения в группу или исключения злонамеренного воздушного судна.
- ***Проверка на правдоподобие.*** Проверка каких-либо параметров на соответствие допустимому поведению. Не являясь необходимой и достаточной, такая проверка тем не менее может указать на «ненормальное» поведение абонента, которое следует более тщательно проанализировать другими методами.

  Можно отметить следующие типы поведения или значения параметров, указывающие на необычность: внезапное появление, заявление о невозможном местоположении, заявление о невозможных параметрах движения, несоответствие планам полета, несоответствие установленным маршрутам и т. п.

- ***Использование дополнительных данных.*** Иногда возникает принципиальная возможность использования дополнительных данных. Например, если для АЗН-В используется ЛПД режима 4, появляется возможность измерения взаимной дальности между абонентами. Такие измерения могут быть использованы для дополнительной верификации.
  Методами пространственной обработки сигналов можно получить угломерные измерения, которые также могут быть использованы для дополнительной верификации.
  Другие возможности могут появиться при модификации существующих и появлении новых протоколов АЗН-В.

ЗАКЛЮЧЕНИЕ

В настоящее время система АЗН-В является уязвимой для угроз кибертеррористического характера. Вместе с тем имеется множество способов повышения защищенности АЗН-В. В статье дана классификация угроз и методов повышения безопасности системы АЗН-В. Ожидается, что в ближайшей перспективе развитие систем наблюдения будет предполагать модернизацию существующего протокола 1090 ES не только с позиции увеличения пропускной способности, но и с целью серьезной переработки в части повышения безопасности, особенно в условиях существующего и развивающегося уровня кибератак. Кроме того, для радикального повышения уровня безопасности модернизироваться должна и сама система ОрВД, использующая данные АЗН-В.

СПИСОК ЛИТЕРАТУРЫ

1. **Костин А.** Спуфинг в воздухе // Хакер. 2013. № 1(168). С. 18–24.
2. **Costin A., Francillon A.** Ghost is in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black Hat, USA. 2012. Pp. 1–12.
3. **McCallie D., Butts J., Mills R.** Security analysis of the ADS-B implementation in the next generation air transportation system // International Journal of Critical Infrastructure Protection. 2011. Vol. 4, Aug., № 2. Pp. 78–87.
4. **Strohmeier M.** Assessing the impact of aviation security on cyber power / M. Smith, M. Schäfer, V. Lenders, I. Martinovic // 8th International Conference on Cyber Conflict (CyCon). NATO CCD COE. 2016. Pp. 223–241.
5. **Strohmeier M.** On perception and reality in wireless air traffic communication security / M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic // IEEE Transactions on Intelligent Transportation Systems. 2017. Vol. 18, Iss. 6. Pp. 1338–1357.
6. **Фальков Э.Я.** Мировой и отечественный курьезы вокруг АЗН-В // Крылья Родины. 2017. № 6–7. С. 34–40.
7. **Фальков Э.Я.** Интеграция беспилотных авиационных систем в общее воздушное пространство: ключевые проблемы и возможные пути решения // Крылья Родины. 2016. № 6. С. 26–32.
8. **Фальков Э.Я., Шаврин С.С.** Кибербезопасность авиационных информационно-связных систем // Радиоэлектронные технологии. 2017. № 5. С. 56–59.
9. **Григорьев И.Д., Орлов В.Г.** Анализ уязвимостей АЗН-В на базе 1090 Extended Squitter // Материалы Международной научно-технической конференции Intermatic-2016. Ч. 5 / МИРЭА. 2016. С. 171–174.
10. **Григорьев И.Д., Орлов В.Г.** Исследование вопросов безопасности системы АЗН-В // Телекоммуникации и информационные технологии. 2016. Т. 3, № 2. С. 53–55.

11. Фадеев А.Н., Орлов В.Г. Особенности обеспечения безопасности в системе АЗН-В ОВЧ ЛПД режима 4 // Материалы Международной научно-технической конференции Intermatic-2015. Ч. 5 / МИРЭА. 2015. С. 297–299.

12. Дуплищева Я.В., Шаврин С.С. Исследование возможности реализации автономной защищенной сети на базе режима VDL-4 // Телекоммуникации и информационные технологии. 2016. Т. 3, № 2. С. 56–58.

13. Strohmeier M., Lenders V., Martinovic I. On the security of the automatic dependent surveillance-broadcast protocol // IEEE Communications Surveys & Tutorials. 2015. Vol. 17, Iss. 2. Pp. 1066–1087.

14. Strohmeier M. Realities and challenges of NextGen air traffic management: the case of ADS-B / M. Schäfer, V. Lenders, I. Martinovic // IEEE Communications Magazine. 2014. Vol. 52, Iss. 6. Pp. 111–118.

СВЕДЕНИЯ ОБ АВТОРАХ

Косьянчук Владислав Викторович, доктор технических наук, профессор, первый заместитель генерального директора ФГУП «Государственный научно-исследовательский институт авиационных систем», vvk@gosniias.ru.

Сельвесюк Николай Иванович, доктор технических наук, профессор РАН, заместитель генерального директора ФГУП «Государственный научно-исследовательский институт авиационных систем», nis@gosniias.ru.

Хамматов Рашит Рифович, кандидат технических наук, доцент, ведущий инженер ФГУП «Государственный научно-исследовательский институт авиационных систем», rrhammatov@2100.gosniias.ru.

AN OVERVIEW OF THE MAIN WAYS TO IMPROVE THE ADS-B SYSTEM SECURITY

Vladislav V. Kosianchuk[1], Nikolai I. Selvesiuk[1], Rashit R. Khammatov[1]
[1]*State Research Institute of Aviation Systems, Moscow, Russia*

The study was conducted with the financial support of the Russian Foundation for Basic Research
Grants № 18-08-463, №18-08-453

ABSTRACT

Automatic dependent surveillance of broadcasting type (ADS-B) is an important means of ensuring the safety and efficiency of air traffic. In the future, the role of ADS-B will increase. At the same time, the cyber security of ADS-B is clearly insufficient. The article analyzes the problem of low security of ADS-B. The main reasons for the vulnerability of ADS-B are the system openness and modern achievements in the development of computer technology and software defined radio (SDR).The classification of probable attacks on the ADS-B system with the goals determination, complexity of implementation and damage from the attack is given. It is concluded that other aviation radio-technical systems possess similar vulnerabilities and require a comprehensive solution to the problem of increasing the security level. The main reasons for insufficient security of aviation communication, navigation and surveillance systems are: long development and certification cycles, legacy and compatibility requirements, price pressure, frequency overloads and the preference for open systems. The paper gives an overview of the main ways to improve the ADS-B system security. It is shown that all methods of improving security can be divided into two groups: methods based on the identification and authentication of broadcast radio networks subscribers and methods based on the verification of data transmitted over broadcast radio networks by unidentified subscribers. The methods of the first group implement algorithms of the "identification-authentication" type and can be divided into non-cryptographic and cryptographic; the latter can use symmetric or asymmetric encryption. The methods of the second group are based on various algorithms for data verification from the ADS-B

system with some additional data obtained through other channels or other sources. The methods of the second group are considered: multilateration, distance restriction, Kalman filtering, statistical hypothesis testing, group verification, reasonableness check and the use of additional data. The article provides the examples of using some methods to improve the security of the ADS-B system, their advantages and disadvantages.

Key words: attack, security, verification, identification, cybersecurity, surveillance, vulnerability, ADS-B.

REFERENCES

1. Kostin, A. (2013). *Spufing v vozdukhe* [Spoofing in the air]. *Khaker* [Hacker], no. 1(168), Pp. 18–24. (in Russian)

2. Costin, A. and Francillon, A. (2012). *Ghost is in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.* Black Hat, USA, Pp. 1–12.

3. McCallie, D., Butts, J. and Mills, R. (2011). *Security analysis of the ADS-B implementation in the next generation air transportation system.* International Journal of Critical Infrastructure Protection, vol. 4, no. 2, Aug., Pp. 78–87.

4. Strohmeier, M., Smith, M., Schäfer, M., Lenders, V. and Martinovic, I. (2016). *Assessing the impact of aviation security on cyber power. 8th International Conference on Cyber Conflict (CyCon).* NATO CCD COE, Pp. 223–241.

5. Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V. and Martinovic, I. (2017). *On perception and reality in wireless air traffic communication security.* IEEE Transactions on Intelligent Transportation Systems, vol. 18, iss. 6, Pp. 1338–1357.

6. Falkov, E.Y. (2017). *Mirovoy i otechestvennyy kuryezy vokrug AZN-B* [World and domestic curiosities around the ADS-B]. Wings of Motherland, no. 6–7, Pp. 34–40. (in Russian)

7. Falkov, E.Y. (2016). *Integratsiya bespilotnikh aviatsionnykh system v obshcheye vozdushnoye prostranstvo: klyuchevyye problemy i vozmozhnyye puti resheniya* [Integration of unmanned aerial systems into the common airspace: key problems and possible solutions]. Wings of Motherland, no. 6, Pp. 26–32. (in Russian)

8. Falkov, E.Y. and Shavrin, S.S. (2017). *Kiberbezopasnost aviatsionnykh informatsionno-svyaznikh system* [Cybersecurity of aviation information and communication systems]. *Radioyelektronnyye tekhnologii* [Radio-electronic technologies], no. 5, Pp. 56–59. (in Russian)

9. Grigoryev, I.D. and Orlov, V.G. (2016). *Analiz uyazvimostey AZN-V na baze 1090 Extended Squitter* [Analysis of vulnerabilities of ADS-B based on 1090 Extended Squitter]. *Materialy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii Intermatic-2016* [Materials of the International Scientific and Technical Conference Intermatic-2016]. *Chast 5* [Part 5]. MIREA, Pp. 171–174. (in Russian)

10. Grigoryev, I.D. and Orlov, V.G. (2016). *Issledovaniye voprosov bezopasnosti sistemy AZN-B* [АЗН-Investigation of safety issues of the ADS-B system]. *Telekommunikatsii i informatsionnyye tekhnologii* [Telecommunication and information technologies], vol. 3, no. 2, Pp. 53–55. (in Russian)

11. Fadeev, A.N. and Orlov, V.G. (2015). *Osobennosti obespecheniya bezopasnosti v sisteme AZN-V OVCH LPD rezhima 4* [Features of security in the system ADS-B VDL mode 4]. *Materialy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii Intermatic-2015* [Materials of the International Scientific and Technical Conference Intermatic-2015]. *Chast 5* [Part 5]. MIREA, Pp. 297–299. (in Russian)

12. Duplishcheva, Y.V. and Shavrin, S.S. (2016). *Issledovaniye vozmozhnosti realizatsii avtonomnoy zashchishchennoy seti na baze rezhima VDL-4* [Investigation of the feasibility of implementing an autonomous secure network based on the VDL-4 mode]. *Telekommunikatsii i informatsionnyye tekhnologii* [Telecommunication and information technologies], vol. 3, no. 2, Pp. 56–58. (in Russian)

13. Strohmeier, M., Lenders, V. and Martinovic, I. (2015). *On the security of the automatic Dependent Surveillance-Broadcast Protocol.* IEEE Communications Surveys & Tutorials, vol. 17, iss. 2, Pp. 1066–1087.

14. Strohmeier, M., Schäfer, M., Lenders, V. and Martinovic, I. (2014). *Realities and challenges of Next Gen air traffic management: the case of ADS-B.* IEEE Communications Magazine, vol. 52, iss. 6, Pp. 111–118.

INFORMATION ABOUT THE AUTHORS

Vladislav V. Kosianchuk, Doctor of Technical Sciences, Professor, First Deputy General Director of FSUE State Research Institute of Aviation Systems, vvk@gosniias.ru.

Nikolai I. Selvesiuk, Doctor of Technical Sciences, Professor RAS, Deputy General Director of FSUE State Research Institute of Aviation Systems, nis@gosniias.ru.

Rashit R. Khammatov, Candidate of Technical Sciences, Associate Professor, Lead Engineer of FSUE State Research Institute of Aviation Systems, rrhammatov@2100.gosniias.ru.

Поступила в редакцию	19.10.2018	Received	19.10.2018
Принята в печать	17.01.2019	Accepted for publication	17.01.2019