DOI 10.53364/24138614_2022_24_1_39
УДК 629.7

Диханова Г., магистрант,
Научный руководитель: **Имашева Г.М**., д.т.н., профессор
АО «Академия гражданской авиации», г. Алматы, РК.

[1]*E-mail: gulnur.dikhanova@gmail.com*
[2]*E-mail: gulnar1507@mail.ru*

ОСНОВНЫЕ СПОСОБЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМЕ АЗН-Б

THE MAIN WAYS TO IMPROVE SECURITY IN THE ADS-B SYSTEM

АТБ-ХТ ЖҮЙЕСІНДЕ ҚАУІПСІЗДІКТІ АРТТЫРУДЫҢ НЕГІЗГІ ТӘСІЛДЕРІ

Аннотация. В этой статье изучается проблемы и способы повышения безопасности в системе ADS-B при утечке и подделке информации.
Ключевые слова: автоматическое зависимое наблюдение-вещания (АЗН-В), безопасность, УВД, воздушное движение, система наблюдения.

Аңдатпа. Бұл мақалада ақпараттың тарап кетуі және жалған болуы кезінде АТБ-ХТ жүйесінің қауіпсіздігін арттыру мәселелері мен әдістері зерттеледі.
Түйін сөздер: Автоматты тәуелді бақылау-хабар тарату (АТБ-ХТ), қауіпсіздік, ӘҚБ, әуе қозғалысы, бақылау жүйесі.

Annotation. This article studies the problems and methods to improve security of the ADS-B system in information leakage and tampering.
Keywords: automatic dependent surveillance-broadcasting (ADS-B), security, ATC, air traffic, surveillance system.

Введение. В настоящее время большинство навигационных систем являются системами наземного базирования. Навигационные средства в основном включают в себя наземное радионавигационное оборудование ILS, VOR, DME и NDB. Системы наблюдения представлены первичными и вторичными радиолокаторами, радиолокационными комплексами, сочетающими первичный и вторичный каналы, а также системами автоматического зависимого наблюдения (АЗН-В). В рамках внедрения перспективных систем наблюдения предприятие расширяет поле наблюдения по технологии АЗН-В. Первичный обзорный радиолокатор (ОРЛ-Т) работает в режиме «по запросу». Системы наблюдения включают в себя 47 средств наблюдения, из них 5 первичных радиолокаторов, 27 вторичных радиолокаторов, 13 комплексов сочетающих первичный и вторичный каналы, 16 систем автоматического зависимого наблюдения (АЗН-В) и 2 радиолокатора обзора летного поля в аэропортах городов Алматы и Астана.

В рамках внедрения перспективных систем наблюдения предприятие внедряет средства автоматического зависимого наблюдения (вещательного типа) (АЗН-В), которые включает в себя автоматический обмен информацией наблюдения между ВС и системой УВД. Данные системы внедрены в 16 аэропортах, что покрывает более 75 % территории Казахстана. Автоматическое зависимое наблюдение в режиме радиовещания (АЗН-В) установлено на

аэродромах: Алматы, Астана, Талдыкорган, Атырау, Актау, Караганда, Балхаш, Жезказган, Костанай, Кызылорда, Павлодар, Тараз, Уральск, Усть-Каменогорск, Семей, Шымкент.[1]

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). Автоматическое зависимое наблюдение радиовещательного типа (АЗН-В) является важным средством обеспечения безопасности и эффективности воздушного движения. В перспективе роль АЗН-В будет увеличиваться. Международная организация гражданской авиации ИКАО включила вопрос о безопасности гражданской авиации в повестку дня в своей «12-й Аэронавигационной конференции», которая рассмотрела кибербезопасность как барьер высокого уровня для внедрения и создала рабочую группу для содействия координации работы заинтересованных сторон.[2] В статье анализируется проблема низкой защищенности АЗН-В. АЗН-В транслирует информацию по открытым и незашифрованным каналам, она уязвима для преднамеренных вторжений и атак, что создает большой риск для безопасности. 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

АЗН-В является методом наблюдения, при котором воздушные суда (ВС) автоматически, по линии передачи данных (ЛПД), передают в центр управления воздушным движением информацию о местоположении и параметрах полета, полученную от бортовых пилотажно-навигационных систем.

АЗН-В позволяет существенно понизить стоимость оборудования средств наблюдения, уменьшить выбросы в атмосферу за счет выбора наиболее эффективных эшелонов полета ВС, потенциально увеличить точность измерения координат, а также получить с борта ВС по линии связи борт-земля дополнительную информацию, позволяющую существенно повысить качество наблюдения и, таким образом, повысить безопасность воздушного движения.

Технология АЗН-В основана на том, что воздушное судно само измеряет свои координаты и другие навигационные параметры и передает их вместе с информацией об идентификации по линии связи «вниз». Эту информацию принимает наземная станция (НС), функции которой – принять сообщения с борта, декодировать, проверить целостность и сформировать выходные сообщения о целях в стандартизированных форматах передачи данных.[3]

В настоящее время стандартизированы три линии передачи данных АЗН-В, которые были предложены, а именно, линия передачи данных (ЛПД) 1090 ES на основе режима S вторичной радиолокации, UAT, VDL-4.

1090 ES и UAT являются наиболее используемыми моделями в настоящее время. Основными преимуществами 1090 ES были названы: единственная линия связи, имеющая выделенный частотный диапазон, наличие на борту антенно-фидерных систем, отсутствие

проблем с электромагнитной совместимостью, возможность использования для независимого измерения координат.

Линия передачи данных UAT была разработана для США из-за высокой загруженности канала 1090 МГц в некоторых регионах, и используется для наблюдения за полетами в нижнем воздушном пространстве. Режим UAT специально разработан для авиационных служб с частотой 978 МГц, и при его применении необходимо установить новое оборудование. Ценой за развертывание второй линии связи стало существенное удорожание наземной инфраструктуры – необходимости двойного покрытия наземными станциями режимов 1090 ES и UAT и взаимной ретрансляции сигналов, а также необходимости оборудования воздушных судов транспондерами UAT.

Линия передачи данных VDL-4 была разработана в Швеции 1980-х годах и так и не была принята в эксплуатацию ни в одной из стран мира. К недостаткам VDL-4 относят проблемы с электромагнитной совместимостью в используемом УКВ диапазоне, невыделенный частотный диапазон и отсутствие возможности для использования сигналов в многопозиционных системах наблюдения. За многие годы пробной эксплуатации АЗН-В 1090 ES в США, Европе и Австралии накоплены многие терабайты данных, которые позволили оценить достоинства и недостатки этой технологии.

Основной довод в пользу развития второй линии передачи данных – это загруженность канала 1090 МГц сигналами вторичной радиолокации, однако основным источником помех для сигналов АЗН-В являются радиолокаторы режима A/C (ATCRBS). Одним из путей уменьшения интенсивности излучения в этом диапазоне является переход на режим S, что также положительно скажется на безопасности воздушного движения.. Еще одним аргументом в пользу использования одной линии передачи данных является имеющийся резерв функциональности сигналов 1090 ES, который позволит увеличить в разы пропускную способность радиоканала (такие работы ведутся на международном уровне), а также наличие зарезервированных для военных целей форматов, которые позволяют реализовать шифрование при передаче данных по каналу 1090 ES.[4]

Данные ADS-B

Передаваемые данные АЗН-В определены в соответствующих стандартах и сертификационных документах. Они включают следующее:

- Горизонтальное положение самолета (широта / долгота)
- Барометрическая высота самолета (такая же как для ВОРЛ)
- Показатели качества
- Идентификация самолета:
  - Уникальный 24-битный адрес самолета
  - Идентификация самолета
  - Код режима A (в случае CS ACNS для «ADS-B Out»)
- Аварийный статус
- SPI (специальный индикатор положения) при выборе

Безопасность. АЗН-В станет объектом исследований, связанных с безопасностью, учитывая его, вероятно, центральную роль в отслеживании воздушных судов и поддержке SAR.

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.

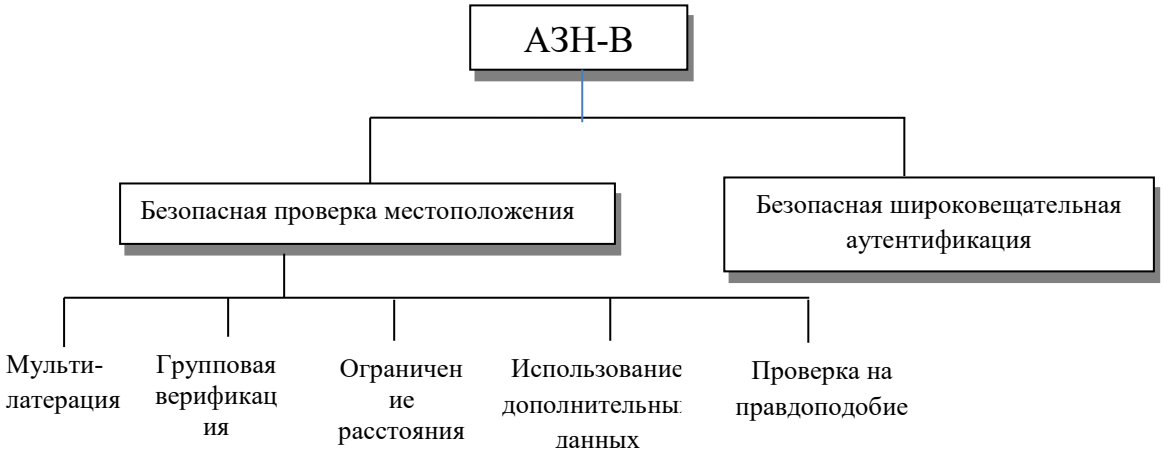
Основные виды атак:

- 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 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 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.[5]

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.

Решение для обеспечения безопасности АЗН-В.

В настоящее время существует два основных типа решений безопасности АЗН-В: безопасная проверка местоположения и безопасная широковещательная аутентификация.[6] На рисунке 1 показана конкретная классификация [7].



• 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). 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.[8]

• 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.[9]

• 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.[10] 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.

• 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.

• 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.

• 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.

Выводы. Безопасность полетов является одним из приоритетов развития гражданской авиации. Способы для повышения безопасности может позволит увеличить защищенность системы АЗН-В от атак и повысить уровень безопасности полетов.

В соответствии с Руководством по управлению безопасностью полётов ИКАО под этим термином понимается состояние, при котором вероятность нанесения вреда человеку или порчи имущества поддерживается на приемлемом уровне или ниже его, что обеспечивается в ходе непрерывного процесса выявления угроз и управления рисками. Конечной целью является полное устранение авиационных происшествий и серьёзных инцидентов, однако в авиационной системе невозможно полностью исключить влияние угроз и связанных с ними рисков. Поэтому необходимо, чтобы риски для безопасности полетов непрерывно уменьшались.

Список использованной литературы

1. Сборник Аэронавигационной информации РК./ Раздел 2. Подчасть 4.1. Радионавигационные средства на маршруте., 2020.

2. K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, and B. M. Phares, ‘‘Cyber security for airports,’’ Int. J. Traffic Transp. Eng., vol. 3, no. 4, pp. 365–376, 2013.

3. E. Atienza, R. Falah, S. García, L. Gutiérrez, M. Á. L. Martínez, and Ó. Robles, ‘‘ADS-B: An air navigation revolution,’’ Rey Juan Carlos Univ.-Fuenlabrada Campus, Madrid, Spain, Tech. Rep., 2013

4. 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.

5. M. Schäfer, V. Lenders, and I. Martinovic, ‘‘Experimental analysis of attacks on next generation air traffic communication,’’ in Applied Cryptography and Network Security. Banff, AB, Canada: Feb. 2013, pp. 253–271.

6. A. Yang, X. Tan, J. Baek, and D. S. Wong, ‘‘A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification,’’ IEEE Trans. Services Comput., vol. 10, no. 2, pp. 165–175, Mar./Apr. 2017.

7. M. Strohmeier, V. Lenders, and I. Martinovic, ‘‘On the security of the automatic dependent surveillance-broadcast protocol,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.

8. N. Xu, R. Cassell, C. Evers, S. Hauswald, and W. Langhans, ‘‘Performance assessment of multilateration Systems–a solution to nextgen surveillance,’’ in Proc. Integr. Commun., Navigat., Surveill. Conf., Herndon, VA, USA, May 2010, pp. D2-1–D2-8.

9. M. R. Manesh and N. Kaabouch, ‘‘Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system,’’ Int. J. Crit. Infrastruct. Protection, vol. 19, pp. 16–31, Dec. 2017.

10. S. Brands and D. Chaum, ‘‘Distance-bounding protocols,’’ in Proc. Theory Appl. Cryptograph. Techn., 1994, pp. 344–359.