УДК 004.491.23

УЯЗВИМОСТИ ADS-B

Стасивский Л.С.[1], Лукьянов Ф.И.[2]
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, stasivskyj@gmail.com[1], lukyanov.f.ua@gmail.com[2]

В данном исследовании рассмотрим более детально, как работают системы управления воздушными потоками старого и нового поколения, а также представим найденные во время его исследования уязвимости и наиболее серьезные риски, связанные с ними. Авиатехнологии находятся на границе нового технического прорыва, и так, как это уже случилось со смартфонами и сетями мобильной связи примерно 5-10 лет назад, новые технологии приводят к новым проблемам. На этот раз – куда более опасным.

Ключевые слова – радиолокаторы; первичные радары наблюдения; вторичные радары наблюдения.

ВВЕДЕНИЕ

Радары (или радиолокаторы) впервые появились в 1940-х годах в военной отрасли. В первую очередь они разрабатывались именно для нужд авиации и морского флота. Применение систем на базе импульсной радиопередачи позволяло определять присутствие в воздухе или на море конкретных физических объектов, а также расстояние до движущихся объектов и воздушный/морской сектор их местонахождения.

ПРИНЦИПЫ РАБОТЫ РАДАРОВ ВОЗДУШНОГО ПОТОКА

На данный момент для целей воздушного наблюдения и управления воздушными потоками существуют два типа радаров:

- первичные радары наблюдения (ПРН, Primary Surveillance Radars или PSR) представляют собой радиолокаторы, которые определяют присутствие воздушных судов при возврате ЭМ-волн в результате отражения от воздушного объекта;
- вторичные радары наблюдения (ВРН, Secondary Surveillance Radars или SSR) широко используются на сегодняшний день для маркировки и отслеживания судов и маршрутов.

Оба типа радаров имеют ряд недостатков. Во-первых – это морально устаревшая технология. Во-вторых, производство и поддержка подобных радаров стоят в 10-20 раз больше, чем оборудование, основанное на новых технологиях. В-третьих, точность обнаружения воздушного судна (далее – ВС) уже не соответствует требованиям и стандартам безопасности и эффективности воздушного движения, а внедрение систем геолокации типа ЄРБ/ГЛОНАСС в ПРН/ВРН либо невозможна, либо очень затратна, либо просто не имеет смысла.

ЧТО ТАКОЕ ADS-B И ЗАЧЕМ ОНА НУЖНА

ADS-B – это акроним от Automatic Dependent Surveillance – Broadcast. Более детально ADS-B расшифровывается как:

- automatic / автоматическое – работает автоматически и не требует вмешательства оператора;
- dependent / зависимое – зависит от системы GPS/ГЛОНАСС;
- surveillance / наблюдение – обеспечивает наблюдение за самолетом;
- broadcast / радиовещание – широковещательная непрерывная радиотрансляция данных всем принимающим на данной радиочастоте приемникам.

Главным пунктом при разработке ADS-B является возможность «видеть» с наибольшей точностью движение воздушных судов благодаря системам позиционирования GPS/ГЛОНАСС. В результате более точного позиционирования воздушных судов удается достичь повышенной безопасности полетов, более компактного и эффективного использования воздушного пространства.

УЯЗВИМОСТИ ADS-B

Данный протокол не использует никаких средств защиты при передаче данных, как, например, шифрование и прочную криптоподпись.

Во всех ADS-B-пакетах присутствуют следующие два поля:

- Aircraft Address (AA), в котором указывается глобально уникальный идентификатор ВС. Аналогично IMSI на SIM-карте или MAC-адресу сетевой карты;
- Parity Information (PI), которое содержит информацию для контроля битной четности, или Parity Information (PI).

Хотя наличие последнего поля, на первый взгляд, предохраняет пакеты от сторонней, случайной или злонамеренной, манипуляции, но это вовсе не так. Данное поле может только подсказать, были ли допущены случайные ошибки при передаче данных. С другой стороны, злоумышленник, вредоносно манипулирующий данными, может просто и легко пересчитать контрольную сумму PI, получая в итоге вполне здоровый и валидный пакет ADS-B. Глобальность идентификатора ВС и уникальность имеют другое последствие – существенно ослабляется безопасность ADS-B с точки зрения конфиденциальности. Очевидно, это позволяет отслеживать данные всех самолетов в режиме реального времени.

Второй тип уязвимостей связан с отсутствием механизмов для прочной криптоподписи. Самое главное в этой уязвимости – это возможность

посылать в эфир поддельные данные или подменивать информацию в настоящих пакетах, а самое неприятное – это тот факт, что сторона, принимающая данные пакеты, не может быть уверена ни в подлинности пакета, ни в идентификации посылающего, ни в отсутствии зловредных изменений в некоем изначально подлинном пакете.

Третий вид уязвимостей связан с отсутствием криптования на пакетном уровне. Систему для ADS-B для применения в мирных целях сделали некриптованной по ряду технических причин. Во-первых, возможности оборудования для ADS-B недостаточны для ресурсоемких криптоопераций. Во-вторых, существуют издержки на уровне менеджмента криптоключей. Если система будет использовать один ключ по системе «shared secret», то его будет достаточно легко вычислить, так как длина пакета невелика и большинство данных в пакете можно предсказать.

СЦЕНАРИИ АТАК НА ADS-B

Например, атака на неконфиденциальность данных и глобально уникальные статические идентификаторы адресов ВС. Перехватывая АА, можно следить исключительно за интересными целями, такими KaKAirForceOne или личные самолеты голливудских звезд. А если все это еще интегрировать с публично доступными базами данных, детально расписывающих личные данные владельцев ВС то естественно, можно получить информацию, показывающую, кто из владельцев (часто миллионеры, звезды, главы корпораций) где находится и куда передвигается. Это в какой-то мере сравнимо с ситуацией, при которой личные данные регистрации автотранспорта станут публично доступными.

Также злоумышленник может сымитировать на экранах диспетчеров полетов воздушное столкновение самолетов или сгенерировать на экранах диспетчеров пару тысяч несуществующих воздушных судов, на базе поддельных данных, но используя реальные идентификаторы других судов, что сделает работу диспетчера практически невыполнимой. Это может привести к разного рода последствиям – от паники в штабе диспетчеров полета до срабатывания наземных систем по предотвращению террористических актов (основанных пока на теоретическом уровне) и вызова срочных аварийных служб.

Исходя из вышеупомянутой информации, положение дел с защищенностью авиасистемы далеко от хорошего, что заставляет задуматься о безопасности полетов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ADS-B (Электрон. ресурс) / Способ доступа: URL: http://ru.wikipedia.org/wiki/ADS-B – ADS-B.

2. СЦЕНАРИИ АТАК НА ADS-I. (Электрон. ресурс) / Способ доступа: URL: http://zip.livejournal.com/88821.html – СЦЕНАРИИ АТАК НА ADS-I.

3. Виртуальная угроза реальным самолетам или уязвимости ADS-B (Электрон. ресурс) / Способ доступа: URL:http://liotcheg.livejournal.com/24613.html – Виртуальная угроза реальным самолетам или уязвимости ADS-B