Назаров Павел Сергеевич

Ст. преподаватель кафедры радиоэлектронных систем, Санкт-Петербургский государственный университет гражданской авиации имени А.А. Новикова

РФ, г. Санкт-Петербург

Лаптев Илья Александрович, Темиров Иван Юрьевич

Студенты, ЛЭГВС 24-02, 2 курс

Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет гражданской авиации имени А.А. Новикова"

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КАНАЛОВ АВИАЦИОННОЙ ЭЛЕКТРОСВЯЗИ НА ОСНОВЕ АЛГОРИТМА ECDSA (Elliptic curve digital signature algorithm)

Аннотация. В статье анализируются актуальные киберугрозы, возникающие в системах авиационной электросвязи, и рассматриваются способы их предотвращения. Основной акцент сделан на криптографической защите информации при обмене данными между воздушными судами и наземными пунктами управления. Предложено использование алгоритма цифровой подписи на эллиптических кривых (ECDSA) для подтверждения подлинности сообщений и контроля их целостности. Описаны особенности применения криптографических методов в авиационных системах, приведены преимущества внедрения ECDSA в коммуникационные протоколы и обозначены перспективы дальнейшего развития технологии.

Ключевые слова: авиационная электросвязь, защита информации, цифровая подпись, ECDSA, аутентификация, безопасность передачи данных, криптография, устойчивость к кибератакам.

Abstract. The paper analyzes modern cyber threats in aviation telecommunication systems and explores ways to prevent them. The main focus is placed on cryptographic data protection during the exchange of information between aircraft and ground control centers. The Elliptic Curve Digital Signature Algorithm (ECDSA) is proposed as a method for message authentication and integrity verification. The features of applying cryptographic technologies in aviation systems are discussed, the benefits of ECDSA integration into communication protocols are highlighted, and future prospects for the technology's development are outlined.

Keywords: aviation telecommunication, information protection, ECDSA, authentication, data security, digital signature, cryptography, cyber resilience.

Современные воздушные перевозки невозможно представить без автоматизированных систем связи и обмена данными. Каналы передачи информации между пилотами и диспетчерами, а также между воздушными судами, обеспечиваются с помощью систем ACARS, CPDLC и ADS-B. Эти технологии позволяют передавать телеметрию, маршруты, отчёты о техническом состоянии и другие важные сведения в реальном времени.

Надёжность и достоверность таких сообщений напрямую влияют на безопасность полётов. Однако открытая структура радиоканалов делает авиационную электросвязь уязвимой перед внешним вмешательством. Распространёнными угрозами становятся спуфинг — подмена сигнала, и джемминг — его глушение. В отдельных случаях злоумышленники могут даже отправлять ложные команды или

искажать навигационные данные, что способно привести к сбоям в управлении воздушным движением.

Поэтому одной из приоритетных задач в авиационной отрасли является создание надёжной системы аутентификации и контроля целостности сообщений. Эффективным решением этой задачи выступает алгоритм цифровой подписи на эллиптических кривых (ECDSA), который сочетает высокий уровень защиты и минимальную нагрузку на вычислительные ресурсы бортового оборудования.

Криптографические методы в авиационной электросвязи решают несколько ключевых задач:

1. подтверждение подлинности источника передаваемых данных;

2. предотвращение несанкционированного изменения или искажения информации;

3. ограничение доступа к данным для третьих лиц.

Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) основан на математике эллиптических кривых. Он использует свойства групповой теории, где каждая точка кривой соответствует уникальному набору координат, а вычисление обратных значений без знания секретного ключа является крайне трудоёмкой задачей.

Принцип работы алгоритма следующий:

1. Создаётся закрытый ключ, который известен только отправителю.
2. На его основе вычисляется открытый ключ, доступный получателю.
3. Каждое сообщение подписывается с использованием закрытого ключа, а на стороне приёмника подпись проверяется по открытому ключу.

Рассмотрим ситуацию, в которой легитимный отправитель подписывает телеграмму ECDSA, злоумышленник пытается отправить поддельное (неподписанное) сообщение — приёмник отвергает его как неаутентичное:

```
# Пример: подпись и проверка ECDSA (использовать: pip install ecdsa)
import hashlib
import base64
from ecdsa import SigningKey, VerifyingKey, NIST256p

# Генерация ключевой пары (однократно)
sk = SigningKey.generate(curve=NIST256p)      # закрытый ключ
vk = sk.verifying_key                          # открытый ключ

# Сериализация ключей (пример сохранения)
priv_pem = sk.to_pem()          # bytes -> хранить приватно
pub_pem  = vk.to_pem()          # bytes -> публикуется или передаётся ЦОМ

# Сообщение (например, ADS-B payload)
message = b"ADS-B: ICAO=ABC123, lat=59.9, lon=30.3, alt=35000"

# Хешируем и подписываем (SHA-256)
# Библиотека ecdsa сама хеширует, но здесь показан явный вариант:
digest = hashlib.sha256(message).digest()
signature = sk.sign_digest(digest)   # результат — байты (r||s) в DER/RAW формат

# Для передачи удобно закодировать в base64
sig_b64 = base64.b64encode(signature).decode('ascii')
print("Signature (base64):", sig_b64)

# -------------------------
# На приёмной стороне — верификация
recv_message = message  # пришло
recv_sig_b64 = sig_b64  # пришла подпись

recv_sig = base64.b64decode(recv_sig_b64)
recv_digest = hashlib.sha256(recv_message).digest()

try:
    vk.verify_digest(recv_sig, recv_digest)
    print("Подпись верна — сообщение аутентично.")
except Exception as e:
    print("Подпись НЕ верна — сообщение отклонено.", e)
```

Рис 1. Демонстрация защиты от спуфинга в авиационной электросвязи с помощью ECDSA (подпись/проверка сообщения на Python).

1. Размер подписи ~64 байта (для P-256) + кодирование — важно учитывать ограничение размера сообщения (особенно для ADS-B). Можно подписывать

только критическую часть сообщения или включать подпись в дополнительный сегмент/телеграмму.

2. Обмен открытыми ключами должен быть защищён: публичные ключи регистрируются и проверяются центром управления (PKI), чтобы предотвращать подмену ключей (man-in-the-middle).

Таким образом, получатель может убедиться, что данные не были изменены и действительно исходят от доверенного источника. При этом вычислительная сложность обратного восстановления закрытого ключа делает систему практически невзламываемой.

Наиболее перспективным направлением применения ECDSA являются протоколы ADS-B, ACARS и CPDLC, которые активно используются в гражданской авиации.

Например, система ADS-B транслирует данные о положении самолёта, скорости и курсе на частотах, доступных для приёма сторонними устройствами. Из-за отсутствия встроенных средств защиты возможно перехватывание и подмена этих сообщений, что может привести к искажению информации о воздушной обстановке.

Интеграция ECDSA позволяет каждой передаче ADS-B сопровождаться цифровой подписью. Диспетчерская система или другой самолёт могут проверить эту подпись, подтверждая, что сообщение поступило от реального источника, а не от стороннего передатчика.

Аналогичный принцип может быть реализован в CPDLC — системе обмена текстовыми сообщениями между пилотом и диспетчером. Использование цифровой подписи ECDSA исключает возможность подделки команд или ложных

указаний, что особенно важно при полётах на больших расстояниях и при работе в автоматическом режиме.

Реализация криптографической защиты возможна как на аппаратном, так и на программном уровне:

1. Аппаратная интеграция — использование специализированных микроконтроллеров и модулей шифрования в бортовой аппаратуре.
2. Программная реализация — добавление функции цифровой подписи в программные стеки связи, например, в протоколах ACARS или LDACS.
3. Наземная верификация — проверка цифровых подписей в центрах управления воздушным движением с последующим анализом подлинности сообщений.

Современные библиотеки, такие как OpenSSL, позволяют интегрировать алгоритм ECDSA даже в ограниченные по ресурсам системы без необходимости полного обновления оборудования. В будущем планируется сочетание ECDSA с квантово-устойчивыми алгоритмами, что обеспечит долговременную защиту данных от атак нового поколения.

Криптографическая защита является неотъемлемой частью развития авиационной электросвязи. С ростом цифровизации воздушного пространства всё большую роль играет надёжная аутентификация сообщений и контроль целостности данных.

Алгоритм ECDSA доказал свою эффективность в информационных технологиях и может стать основой для создания безопасных каналов связи между пилотом и диспетчером. Его внедрение позволит минимизировать риск подмены

данных, повысить доверие к системам ADS-B и CPDLC, а также обеспечить устойчивость авиационной инфраструктуры к кибервоздействиям.

Таким образом, интеграция ECDSA в авиационные протоколы электросвязи является важным шагом на пути к формированию единого защищённого пространства воздушных коммуникаций, где безопасность информации напрямую связана с безопасностью полётов.

Список использованных источников

1. Koblitz N. Elliptic Curve Cryptosystems. Mathematics of Computation, 1987, pp. 203–209.

2. Menezes A., Vanstone S., Oorschot P. Handbook of Applied Cryptography. CRC Press, 1996, pp. 315–420.

3. Miller V. Uses of Elliptic Curves in Cryptography. Advances in Cryptology – CRYPTO’85 Proceedings, 1986, pp. 417–426.

4. National Institute of Standards and Technology (NIST). FIPS PUB 186-4: Digital Signature Standard (DSS), 2013.

5. ICAO. Manual on System Wide Information Management (SWIM). Doc 10039, 2020.

6. Strohmeier M. Security in Next Generation Air Traffic Communication Networks. IEEE Communications Magazine, 2018.