

РЕАЛИЗАЦИЯ ПЕРЕДАЧИ ВИДЕОПОТОКА НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ

Дудкин А.С. (ВКА), Зыков В.В. (ВКА), Яковлев В.М. (ВКА),

Научный руководитель – кандидат технических наук, доцент Дудкин А.С.
(Военно-космическая академия имени А.Ф.Можайского)

Введение. Современные технологии сбора и обработки видеопотока играют ключевую роль в различных сферах, включая мониторинг инфраструктуры, транспортных потоков, доставку грузов, фиксация различного рода нарушений и прочее, обеспечивая эффективное выполнение задач, которые ранее требовали значительных ресурсов и времени. Однако с увеличением их применения возникает критически важный вопрос безопасности передаваемого видеопотока. Данные системы часто передают конфиденциальные видеозаписи, содержащие важную информацию о местоположении, действиях и событиях. Перехват или несанкционированный доступ к этому видеопотоку может иметь серьезные последствия, включая утечку государственных или коммерческих данных, нарушение приватности и даже угрозу национальной безопасности. Поэтому для защиты видеоданных, передаваемых по беспроводным каналам, крайне важно применять надежные методы шифрования. Эффективное шифрование гарантирует, что даже в случае перехвата, видеопоток останется недоступным для злоумышленников. Современные технологии шифрования позволяют защитить как сам видеопоток, так и каналы связи между устройством и оператором, создавая надежный барьер от потенциальных угроз. Таким образом, внедрение высококачественного шифрования становится не просто необходимостью, а важным шагом к обеспечению безопасности и конфиденциальности в эпоху цифровых технологий, где защита информации имеет первостепенное значение.

Основная часть. С целью организации шифрования при передаче видеопотока, полученного от системы видеонаблюдения, необходимо разобраться с некоторыми ключевыми моментами:

- какой метод шифрования будем использоваться?
- с помощью чего лучше организовать передачу видеопотока?
- каким образом добиться хорошего качества передаваемого видеопотока?

Существует несколько методов шифрования данных, полученных с видеоустройств. Каждый из них имеет свои особенности и применяется в зависимости от требований к безопасности, производительности и типу передаваемых данных:

1. AES (Advanced Encryption Standard): один из самых популярных симметричных алгоритмов шифрования [1].

2. RSA (Rivest-Shamir-Adleman): асимметричный алгоритм шифрования, который используется для безопасного обмена ключами [2].

3. ECC (Elliptic Curve Cryptography): еще один метод асимметричного шифрования, который использует эллиптические кривые для создания ключей [3].

4. ChaCha20-Poly1305: современный алгоритм шифрования, который сочетает в себе потоковое шифрование ChaCha20 и аутентификацию Poly1305 [4].

Организация передачи видеоданных требует выбора подходящих технологий, которые обеспечат надежность, скорость и качество передачи:

1) Wi-Fi: подходит для локальных задач, обеспечивая стабильное соединение на коротких расстояниях. Wi-Fi может быть использован для передачи данных в пределах видимости устройства и его оператора.

2) Bluetooth: подходит для передачи данных на очень короткие расстояния, например, для передачи данных между мобильными устройствами оператора.

3) Специализированные радиочастотные каналы: использование частот, специально выделенных для авиационных и телекоммуникационных устройств, может обеспечить надежную и защищенную передачу данных (Race Band, Low Band и т.д.) [5].

4) Системы передачи данных на основе спутниковой связи: обеспечивают глобальное покрытие, что делает их идеальными для работы в удаленных или труднодоступных районах [6].

5) Mesh-сети: позволяют создавать сеть из нескольких дистанционно управляемых устройств и наземных станций, что обеспечивает надежную передачу данных даже в условиях плохого сигнала. Mesh-сети могут автоматически перенаправлять данные через доступные узлы, что увеличивает устойчивость системы [7].

Для обеспечения высокого качества видеопотока необходимо оптимизировать кодирование и сжатие видео. Использование современных кодеков, таких как H.264 или H.265, позволяет эффективно сжимать данные без значительной потери качества. Эти кодеки обеспечивают высокую степень сжатия, что особенно важно при передаче видеопотока с мобильных устройств, где ограниченная пропускная способность может стать серьезной проблемой.

Выводы. Комплексный подход к шифрованию, выбор технологий передачи и оптимизация качества видеопотока являются ключевыми факторами для успешного использования современных устройств в различных условиях. Это не только повышает уровень безопасности и конфиденциальности, но и способствует более эффективному выполнению задач, что делает такие системы важным инструментом в современном мире.

Список использованных источников:

1. Cryptography and Network Security: Principles and Practice [Электронный ресурс]. – URL: <https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security-principles-and-practice-7th-global-edition.pdf> – (дата обращения 01.01.2025).
2. Applied Cryptography [Электронный ресурс]. – URL: <https://mrajacse.wordpress.com/wp-content/uploads/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf> – (дата обращения 01.01.2025).
3. Elliptic Curve Cryptography for Dummies 1 [Электронный ресурс]. – URL: <https://www.smalsresearch.be/elliptic-curve-cryptography-tutorial1/> – (дата обращения 01.01.2025).
4. RFC 7539 (ChaCha20 and Poly1305) [Электронный ресурс]. – URL: <https://datatracker.ietf.org/doc/html/rfc7539> – (дата обращения 01.01.2025).
5. Видеолинк [Электронный ресурс]. – URL: <https://rsearch.ru/wiki/Видеолинк> – (дата обращения 01.01.2025).
6. Satellite Communications [Электронный ресурс]. – URL: https://www.srecwarangal.ac.in/ece-downloads/IV_II_satellite_communications_by_dennis_roddy4thedition.pdf – (дата обращения 01.01.2025).
7. Mesh-сети стандарта IEEE 802.11s – технологии и реализация [Электронный ресурс]. – URL: https://www.lastmile.su/files/article_pdf/2/article_2099_241.pdf – (дата обращения 01.01.2025).