КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Берёзкин Р.В.

Власова Г.А. – к.т.н., доцент

В работе рассматриваются основные факторы, которые необходимо учитывать при обеспечении защиты передачи видеоинформации. Рассматриваются алгоритмы шифрования для защиты передаваемых данных и пакетов данных сетевого видеонаблюдения.

Системы видеонаблюдения делят на аналоговые и сетевые. В данной работе было выбрано сетевое видеонаблюдение, так как оно даёт быструю передачу данных, лучшее качество сигнала, помехозащищённость, такую систему проще масштабировать, а также стоит учесть то, что хранение, просмотр и обработка информации производится, в большинстве случаев, для данных в цифровом формате.

IP-наблюдение успешно интегрируется в системы безопасности крупных и мелких объектов, а монтаж IP-видеонаблюдения прост и доступен – система легко передислоцируется и переформатируется под решение новых технических задач без дополнительной прокладки кабельных коммуникаций.

Есть несколько уровней защиты для обеспечения безопасной передачи и данных по сетям. Первый уровень - это авторизация и аутентификация. Пользователь или устройство идентифицирует себя в сети и на удаленном устройстве при помощи имени пользователя и пароля, которые проверяются, и по результатам проверки устройство получает доступ или не получает, соответственно. Для повышения безопасности данные шифруются. Наиболее распространенными методами шифрования считаются SSL/TLS (так же известный как HTTPS), VPN и WEP или WPA в беспроводных сетях. При использовании шифрования скорость передачи данных может в некоторой степени уменьшиться в зависимости от метода шифрования и его реализации.

Дополнительным средством защиты предусматривают возможность создания списка разрешенных сетевых адресов (так называемая фильтрация сетевых адресов).

Протокол HTTPS это метод шифрования, когда передаваемые данные упаковываются в криптографический протокол SSL или TLS. Это означает, что происходит шифрование самих передаваемых данных и протокола HTTP.

Чтобы сетевой видеокамере было разрешено передавать данные по безопасному протоколу HTTPS, у нее или него должен быть цифровой сертификат и ассиметричная ключевая пара. Пара ключей генерируется устройством. Сертификат генерируется или самостоятельно подписывается устройством, или выдается сертификационным органом. При использовании протокола HTTPS сертификат используется для аутентификации и шифрования. Это означает, что браузер проверяет видеокамеру по сертификату, и сертификат используется алгоритмом шифрования с открытыми ключами.

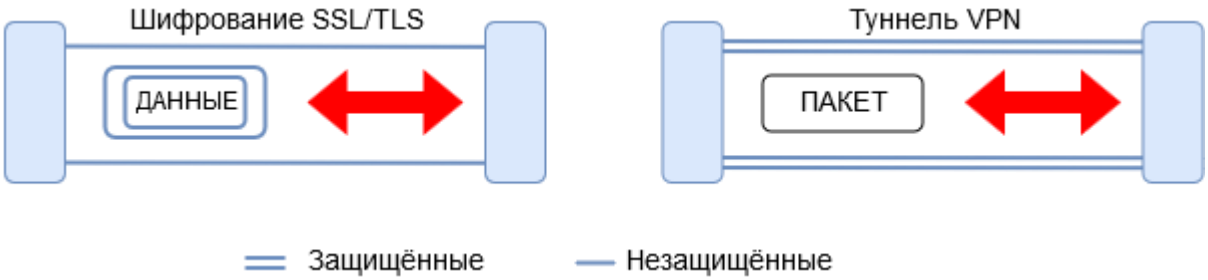

Рис. 1 – Сравнение шифрования с применением протоколов SSL/TLS и сети VPN.

Виртуальная частная сеть (VPN) позволяет организовать защищенный "канал" между двумя обменивающимися данными устройствами, таким образом, обеспечивая безопасный и защищенный обмен данными через Интернет. В этом случае происходит шифрование всего пакета, включая его данные и заголовок, который содержит сведения об источнике и адресе назначения, типе пересылаемой информации, порядковом номере пакета в последовательности пакетов и длине пакета.

Данные средства защиты имеют широкое применение, но находятся в стадии постоянного развития, так как имеют место случаи взломов и обнаружения уязвимостей.

Список использованных источников:
1. Техническое руководство по сетевому видеонаблюдению: [Электронный ресурс]. – Режим доступа: https://www.axis.com/ru-ru/learning/web-articles/technical-guide-to-network-video/.
2. Дамьяновски В. CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии. /Пер, с англ. – М.: ООО «Ай-Эс-Эс Пресс», 2006, – 480 с.