Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Берёзкин
Роман Валерьевич

Методика проектирования устройств криптографической защиты информации для системы видеонаблюдения «умного дома» (автоматизированного жилого помещения)

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-39 81 03 «Информационные радиотехнологии»

_____
(подпись магистранта)

Научный руководитель
Г. А. Власова_____
(фамилия, имя, отчество)
к.т.н., доцент_____
(ученая степень, ученое звание)

_____
(подпись научного руководителя)

Минск 2018

ВВЕДЕНИЕ

Система видеонаблюдения в контексте «умный дом» представляет собой программно-аппаратный комплекс, который предназначен для организации визуального наблюдения и контроля других устройств системы «умный дом». Самая очевидная задача - это обеспечить безопасность объекта (внутренних и наружных помещений, которые прилегают к территории и др.), людей, материальных и интеллектуальных ценностей, путем круглосуточного видеонаблюдения и контроль событий в порядке реального времени и разбора архивированной информации.

При необходимости дополнительного обеспечения безопасности используют системы видеонаблюдения, которые, как правило, интегрируются в комплексные системы безопасности. Такие комплексы фиксируют, записывают и анализируют информацию, поступающую от видеокамер, считывателей системы контроля доступа, охранных датчиков, а также «принимают решения» по защите охраняемого объекта в автономном режиме или по указанию оператора системы.

Сетевое видеонаблюдение, равно как и другие виды передачи данных, например, электронная почта, сетевой серфинг и IP-телефония, осуществляется по проводным и беспроводным сетям (по протоколу IP). Цифровые аудио- и видеосигналы передаются по той же сети, что и остальные данные. Сетевое видеонаблюдение предлагает множество преимуществ по сравнению с традиционными аналоговыми системами видеонаблюдения (CCTV), особенно когда речь идет об охране и обеспечении безопасности.

Такая система может быть открытой или защищенной в той мере, в какой это необходимо. Многие пользователи хотят иметь доступ к изображению в режиме реального времени, чтобы его могли просматривать члены семьи, друзья. Однако охранные системы необходимо защищать от несанкционированного доступа как извне, так и изнутри.

Реализация системы видеонаблюдения на основе стандартной сетевой инфраструктуры имеет множество преимуществ. Установка и обслуживание становятся менее затратными, поскольку общие ресурсы распределяются между несколькими системами, в том числе для передачи голоса по IP (VoIP), управления зданием и т.д. У видеосистем на базе IP к тому же нет ограничений по разрешению и частоте кадров, которые присущи аналоговым системам. Практически все видеокамеры и видеокодеры поддерживают технологию питания по сети (PoE), поэтому не требуют отдельных кабелей питания, а значит, такие видеокамеры проще устанавливать.

Управление видеокамерами и видеопотоками стало значительно проще. Спектр поддерживаемых современных функций видеонаблюдения постоянно расширяется. На рынке имеется широкий выбор специализированного программного обеспечения для самых разных систем видеонаблюдения, начиная от небольших систем, насчитывающих несколько видеокамер и устанавливаемых в магазинах, и заканчивая огромными системами, в состав которых входят сотни видеокамер, установленных зачастую на нескольких объектах, географически разнесенных друг от друга.

Расширяющиеся возможности видеонаблюдения дают новые средства для деятельности злоумышленников. Необходимо принять меры защиты передачи информации от видеокамеры клиентскому приложению и обратно.

Целью настоящей работы является исследование и обоснование оптимальной методики проектирования устройств криптографической защиты информации для системы видеонаблюдения автоматизированного жилого помещения.

Достижение поставленной цели требует решения следующих задач:

- выполнить анализ существующих методов защиты информации;
- определить параметры методов защиты информации, обеспечение которых наиболее важно, учитывая специфику систем видеонаблюдения;
- выбор и оптимизация алгоритмов криптографической защиты в соответствии со спецификой функционирования системы видеонаблюдения.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель работы: исследование и обоснование оптимальной методики проектирования устройств криптографической защиты информации для системы видеонаблюдения автоматизированного жилого помещения.

Задачи исследования: анализ алгоритмов криптографической защиты информации для систем видеонаблюдения, являющихся частью IoT. Выбор и оптимизация устройства криптографической защиты в соответствии со спецификой функционирования системы видеонаблюдения.

Объект исследования: системы видеонаблюдения и устройства криптографической защиты информации.

Предмет исследования: системы видеонаблюдения автоматизированного жилого помещения, алгоритмы малоресурсной криптографии.

Актуальность: актуальность работы вызвана доступностью массовому потребителю различного рода электронных устройств с подключением к сети Интернет. Эта тенденция приводит к появлению новых угроз для информации пользователей подобных устройств.

Материалы диссертации выкладывались в тезисном виде на 54-й научной конференции аспирантов, магистрантов и студентов БГУИР и на 16-ой Белорусско-российской научно-технической конференции «Технические средства защиты информации».

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении показано, в чём заключается научная новизна, теоретическая и практическая значимость работы.

В главе 1 описываются особенности систем видеонаблюдения, необходимость криптографической защиты и простейшие средства защиты подобных систем.

В главе 2 описываются особенности малоресурсных алгоритмов криптографии, сделан обзор и систематизация существующих алгоритмов. Проанализированы и, в дальнейшем, выбраны блочные шифры для выполнения поставленной задачи.

В главе 3 легковесные алгоритмы шифрования анализируются исходя из требований к криптографической защите систем видеонаблюдения. Два выбранных алгоритма программно и аппаратно моделируются для исследования на быстродействие. Сделан вывод о параметрах блочных шифров, влияющих на быстродействие и сложность реализации.

В приложениях приведены коды программных реализаций алгоритмов шифрования, выбранных в Главе 3.

ВЫВОДЫ

В результате проведённых исследований получены следующие результаты.

Задачей данной работы являлся анализ алгоритмов криптографической защиты информации для систем видеонаблюдения, являющихся частью IoT, выбор и оптимизация устройства криптографической защиты в соответствии со спецификой функционирования системы видеонаблюдения

Для выполнения поставленных задач были изучены современные системы видеонаблюдения, изучены и оптимизированы легковесные алгоритмы блочного шифрования. На основе изученных материалов был написан программный код, реализующий два, наиболее подходящих для поставленной задачи, алгоритма. Также была изучена аппаратная реализация алгоритмов шифрования.

Данные, полученные в результате исследований, доказали, что выбранные алгоритмы PRESENT и CLEFIA соответствуют требованиям, поставленным для алгоритмов шифрования, применяемых для криптографической защиты систем наблюдения автоматизированных жилых помещений. Выбранные алгоритмы обеспечивают требуемый уровень защиты и скорости шифрования, обладая при этом малыми требованиями к вычислительным способностям устройства. Обозначена специфика применения каждого алгоритма.

Представленные в работе исследования и выводы будут способствовать ускорению разработки и повышению надежности систем видеонаблюдения, являющихся частью IoT.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А.] Берёзкин Р.В. Криптографическая защита информации в системах видеонаблюдения / Р.В. Берёзкин, Г.А. Власова //54-ая научно-технической конференция аспирантов, магистрантов и студентов БГУИР – Минск, 2018.

[2-А.] Берёзкин Р.В. Аспекты применения криптографической защиты информации в системах видеонаблюдения / Р.В. Берёзкин, Г.А. Власова // 16-ая Белорусско-российская научно-техническая конференция «Технические средства защиты информации» – Минск, 2018.