ОСОБЕННОСТИ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ДАТЧИКОВ И ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ В СИСТЕМЕ «УМНЫЙ ДОМ»

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

Войтехович С.А.

Власова Г.А. – к.т.н., доцент

В статье рассмотрены основные угрозы функционирования интеллектуальных систем «Умный дом», представлено сравнение наиболее распространенных сетевых стандартов KNX, LonWorks и BACnet. Рассмотрены основные направления криптографической защиты данных в системах «Умный дом», в том числе способы защиты систем автоматизации на базе специальных криптографических надстроек, решения в области малоресурсной (легковесной) криптографии.

Системы «Умного дома» или автоматизированного здания присутствуют почти во всех областях жизнедеятельности человека. В том числе и на важных промышленных объектах: атомных станциях, нефтеперерабатывающих заводах, газопроводах. Автоматизированные системы управления (АСУ) предназначены для управления и мониторинга различных элементов автоматики. Они включают в себя управление электропитанием, сигнализацией, освещением, видеонаблюдением, системами кондиционирования, подачей тепла и т.д. АСУ обеспечивают защиту от несанкционированного вторжения на территорию здания или открытые территории благодаря системам контроля доступа. Однако сами системы автоматизации нуждаются в информационной защите.

Современные информационные технологии являются важнейшей составляющей любого «Умного дома», они играют активную роль в функционировании всех его компонентов. Так, энерго- и водоснабжение «Умного дома» предполагает использование интеллектуальной системы учета и удовлетворения спроса на электроэнергию и воду, программно-аппаратного комплекса управления интеллектуальной энергосетью, водоснабжением и водоотведением. Аналогичная ситуация — с управлением системами безопасности (видеонаблюдение, видеофиксация, система оповещения, система обеспечения вызова экстренных оперативных служб). Повсеместное и непрерывное использование информационных технологий обуславливают высокую степень уязвимости интеллектуальной системы «Умный дом» перед возможными сбоями функционирования.

Потенциальными носителями угрозы сбоя функционирования из-за ошибок в программном обеспечении являются его разработчики. К угрозам сбоя функционирования системы вследствие внешних проблем с оборудованием можно отнести его хищение обслуживающим персоналом или злоумышленниками; неумышленный или умышленный вывод из строя (уничтожение) оборудования, а также носителей данных. К угрозам сбоя функционирования системы вследствие проблем с данными относятся порча данных, их модификация при разрешенном доступе (обслуживающий персонал); как умышленные, так и неумышленные ошибки ввода; искажение данных и ввод ложной информации при несанкционированном доступе. К угрозам сбоя функционирования системы вследствие нарушения информационного обмена можно отнести блокирование (установка помех, закладок) каналов связи, проходов, задержку передачи информации (замедление, выставление дополнительных требований, пауза); выход системы из штатного режима эксплуатации вследствие случайных или преднамеренных действий обслуживающего персонала, пользователей, злоумышленников (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т. д.).

Высокая уязвимость информационной системы «Умный дом» и значительная потенциальная опасность последствий, которые могут возникнуть в результате сбоев ее функционирования, делают очень актуальной и важной проблему обеспечения защиты данных в интеллектуальных системах «Умный дом», в том числе криптографическую [1].

В качестве основных направлений предотвращения угроз безопасности интеллектуальных систем типа «Умный дом» чаще всего называют стандартизацию протоколов беспроводной передачи данных в распределенных сетевых инфраструктурах, использование гомоморфных алгоритмов шифрования информации, а также защиту содержания зашифрованных пакетов данных в облачных сервисах. Выработан и ряд базовых правил, которые позволяют защитить интеллектуальные системы. К ним можно отнести разделение сети Интернет и сети «Умного дома», а также запрет на установку таких небезопасных функций, как, например, управление по SMS [2].

По мнению некоторых специалистов, в частности, А.Г. Бельтова, А.В. Новицкого, В.Н. Конева, М.И. Фомина, В.Л. Евсеева, С.Д. Фесенко, безопасность стандартов автоматизации целесообразно рассматривать на базе следующих важнейших стандартов: возможность проведения аутентификации, проверка целостности и проверка принимающей стороны (конфиденциальность) [3].

В таблице 1 представлено сравнение наиболее распространенных сетевых стандартов KNX, LonWorks и BACnet по данным параметрам безопасности. Проверка аутентификации необходима для того, чтобы ограничить доступ к штатному контролеру, который может отправлять в сеть управляющие команды, и не дать злоумышленникам возможности управления сетью автоматизации.

Таблица 1 - Сравнение сетевых стандартов

	Аутентификация	Целостность	Конфиденциальность
KNX	32-бит пароль	-	-
LonWorks	64-бит MAC 48-бит ключ	64-бит MAC 48-бит ключ	-
BACnet	DES	DES	DES

Проверка целостности необходима для защиты уже отправленных сообщений от их несанкционированных изменений. Параметр конфиденциальности означает невозможность для злоумышленника, подключившегося к сети, отправлять сообщения, которые могут восприниматься и приниматься к исполнению сетевыми устройствами.

По параметрам безопасности лучшие показатели — у стандарта BACnet. В KNX единственным защитным механизмом является предотвращение несанкционированного доступа к управляющим службам с помощью текстовых паролей. В LonWorks помимо параметра аутентификации контролируется также параметр целостности. Данный протокол имеет механизм для идентификации отправителя и контроля целостности данных — четырех- шаговый «оклик-отзыв», основанный на хеш-функции, с помощью которой шифруется 64-битный MAC-код (Message Authentication Code) на 48-битном секретном ключе. Однако из-за малой длины ключа функцию нельзя признать надежной. В BACnet все три параметра безопасности (аутентификация, целостность и конфиденциальность) достигаются благодаря симметричному алгоритму шифрования DES (Data Encryption Standard). К сожалению, данный алгоритм также не является безопасным — уже несколько лет в открытом доступе публикуются работы, посвященные его взлому. Для обеспечения надежной информационной защиты интеллектуальных систем типа «Умный дом» необходимо использовать, помимо остальных, способы защиты систем автоматизации на базе специальных криптографических надстроек. Некоторые специалисты предлагают использовать их на базе протокола KNX путем замены разветвителей на спроектированные с реализацией защищенных функций, в т. ч. по генерации, раздаче, ограничению времени действия и аннулированию ключей. Защита систем «Умный дом» – не простая задача. Сложность заключается в том, что многие протоколы, представленные на рынке, изначально не были спроектированы с учетом возможных атак со стороны злоумышленников [4].

С развитием интеллектуальных систем типа «Умный дом» возрастает также и значение так называемой малоресурсной (легковесной) криптографии (lightweight cryptography, LWC), под которой понимается раздел криптографии, имеющий своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами (память, электропитание, размеры) для функционирования [5].

Как правило, к реализации малоресурсной криптографии предъявляют следующие требования: малые размеры микросхемы, обработка небольших потоков информации с приемлемым быстродействием, дешевизна устройств. При этом криптостойкость должна снижаться незначительно. Однако легко реализовать две из трёх целей разработки, но очень трудно оптимизировать все три цели такой разработки одновременно [6].

Следует отметить, что к настоящему времени не найдено решение в области малоресурсной криптографии, которое подходило бы для использования в различных приложениях — и RFID, и бесконтактных смарт-картах, и сенсорах и др. По мнению ряда экспертов, направление малоресурсной криптографии будет одним из определяющих в развитии криптографии в ближайшие годы [7].

К направлениям защиты данных в интеллектуальных системах типа «Умный город» можно отнести также такие, как автоматизация поиска уязвимостей с помощью обратной трассировки графа передачи управления; обеспечение безопасности гетерогенных систем с применением гомоморфной модулярной криптографии; система распределенной аутентификации на основе изогений эллиптических кривых; оценка безопасности киберфизических систем на основе фрактальных методов и др.

Список использованных источников:

8. Глобальные технологические тренды / Институт статистических исследований и экономики знаний НИУ ВШЭ // Сайт НИУ «Высшая школа экономики». 2016. URL: https://issek.hse.ru/trendletter/news/172112565. html.

9. Бельтов, А.Г., Новицкий А.В. и др. Анализ уязвимостей технологий автоматизации умного дома // Спецтех-ника и связь. — 2012. — № 4.

10. Стариковский А.В., Жуков И.Ю. и др. Исследование уязвимостей систем умного дома // Спецтехника и связь, 2012. — № 2.

11. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2005.

12. Кяжин, С.Н., Моисеев А.В. Криптография в облачных вычислениях: современное состояние и актуальные задачи // Безопасность информационных технологий. — 2013. — № 3.

13. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. Вып. №1.

14. Криптография в эпоху облаков и всеобщей связности // Сайт конференции «РусКрипто». 2016. URL: http:// www. ruscrypto.ru/press-center/publications/2012–05–31. html.