Яров П.В., Чернышев О.Л. Информационная безопасность систем “Умный дом”. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVI Междунар. научно-техн. конф. – Пенза: ПДЗ, 2016. – С. 228-230.

УДК 681.51

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ «УМНЫЙ ДОМ»

П.В. Яров, О.Л. Чернышев

INFORMATION SECURITY OF «SMART HOUSE» SYSTEMS

P.V. Yarov, O.L. Chernyshev

Аннотация. Рассмотрена информационная безопасность систем «Умный дом». Проведен анализ возможных уязвимостей и рассмотрены методы их устранения.

Ключевые слова: безопасность, умный дом, уязвимость, защита.

Abstract. As part of the article, deals with information security of «Smart House» systems. The analysis of existing vulnerabilities and describes possible ways to address them.

Keywords: security, smart house, protection, rating, vulnerability.

В настоящее время системы «умного дома» охватывают многие области жизни современного человека. Такие системы зачастую присутствуют и на важных промышленных объектах, таких как: атомные станции, электростанции, нефтеперерабатывающие заводы, газопроводы. Системы «умного дома» предназначены для мониторинга и управления различными элементами автоматики. Они включают в себя управление кондиционированием, освещением, видеонаблюдением, электропитанием, а также обеспечивают защиту от несанкционированного вторжения.

Условно всю систему «умного дома» можно поделить по функциональному назначению на следующие компоненты [1].

1. Источник питания. В качестве питания обычно используются аккумулятор с возможностью подключения к сети переменного тока 220 В.
2. Управляющее устройство. Микроконтроллерное устройство, связывающее систему в целом, генерирующее управляющие сигналы, собирающее информацию с датчиков.
3. Входные устройства – сенсоры. К сенсорам можно отнести датчики температуры, освещения, влажности и т.д.
4. Активаторы – выходные устройства. Простейшие активаторы представляют собой реле и могут только включать и выключать нагрузку. Более сложные устройства способны регулировать ток, отдаваемый в нагрузку. Такие активаторы могут регулировать яркость любого типа ламп. Отдельную группу активаторов составляют устройства, управляющие, например, жалюзи.
5. Устройства связи с управляющим устройством и другими информационными системами. Среди них наиболее часто используются Blue-tooth, Wi-fi, GSM-модули.

Защита систем умного дома – сложная задача. Сложность заключается в том, что большинство протоколов, представленных на рынке, изначально не были спроектированы с учетом возможных атак со стороны мошенников. Применение хорошо зарекомендовавших себя в IT-сфере механизмов, например, SSL (Secure

Socket Layers – уровень защищенных сокетов) / TLS (Transport Layer Security – безопасность транспортного уровня) или VPN (Virtual Private Network – виртуальная частная сеть), невозможно из-за ограниченности ресурсов устройств, подключаемых к системе автоматизации (внутренняя память, вычислительные мощности). Поэтому среда передачи данных, как правило, является самым уязвимым местом в области безопасности систем автоматизации [3].

При проектировании систем «умного дома» нужно уделить особое внимание информационной безопасности. Существует ряд базовых правил:

- разделить сеть Интернет и сети «умного дома»;
- отключить от управления системой жизненно важные функции здания;
- не устанавливать небезопасные функции, например, управление по SMS и т.д.

Однако соблюдение базовых правил безопасности не гарантирует безопасность системы. Дело в том, что стандарты автоматизации имеют низкий уровень защиты. Поэтому необходимо учесть ряд важных параметров системы:

1. Ограничение доступа к центральному контроллеру, который отправляет управляющие команды. Чтобы избежать проблемы несанкционированного доступа к системе, необходимо учесть ряд важных аспектов: проверка достоверности источника, проверка целостности дейтаграмм, проверка принимающей стороны. Конфиденциальность необходима, чтобы только авторизованные устройства могли отправлять данные центральному контроллеру. Проверка целостности дейтаграмм нужна для того, чтобы мошенник не мог изменить уже отправленное сообщение, подставив свои параметры [3].

2. Использование алгоритмов шифрования. Чтобы избежать утечки конфиденциальных данных, а также скрыть реализацию системы команд устройства.

3. Реализация нескольких режимов защиты данных. Дело в том, что при передаче пользовательских данных достаточно удовлетворять требованиям защиты целостности данных, а также обеспечения их достоверности, а при передаче управляющих команд нужно обеспечить защиту от пересылки перехваченных сообщений. Операция XOR над выходными данными со 128-разрядного счетчика после операции XOR с данными дейтаграммы позволяет гарантировать уникальность каждого сообщения[4].

Подводя итог, можно отметить, что при разработке систем «умный дом» нужно уделить особое внимание информационной безопасности. В ходе реализации такой системы необходимо не только уделить внимание базовым принципам защиты, но и ограничить доступ к центральному контроллеру, использовать алгоритмы шифрования, а также реализовать несколько режимов защиты данных.

Библиографический список

1. Стариковский А.В., Жуков И.Ю., Михайлов Д.М., Толстая А.М., Жорин Ф.В., Макаров В.В., Вавренюк А.Б. Исследование уязвимостей систем умного дома // Спецтехника и связь. 2012. № 2. С. 55–57.

2. Чернышев О.Л. Особенности нейтрализации информационных воздействий: информационно-технический аспект // Информационные ресурсы и системы в экономике, науке и образовании: сб. статей V Междунар. конф. Пенза: ПДЗ, 2015. С. 102–107.

3. Дитрих Д., Кастнер В., Саутер Т., Низамутдинов О. EIB – система автоматизации зданий. Пермь: ПермГТУ, 2001. 378 с.

4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.

Яров Павел Владимирович
Тверской государственный
технический университет,
г. Тверь, Россия
E-mail: yarov.pavel@mail.ru

Yarov P.V.
Tver State Technical University,
Tver, Russia

Чернышев Олег Леонидович
Тверской государственный
технический университет,
г. Тверь, Россия
E-mail: plumber63@mail.ru

Chernyshev O.L.
Tver State Technical University,
Tver, Russia