А. В. Стариковский, И. Ю. Жуков, М. И. Фомин, Д. М. Михайлов, А. Б. Вавренюк

ИССЛЕДОВАНИЕ ВОЗМОЖНЫХ УЯЗВИМОСТЕЙ СИСТЕМЫ «УМНОГО ДОМА», ПОСТРОЕННОЙ НА ТЕХНОЛОГИИ X10

Сегодня системы автоматизированного управления зданиями, или системы «умного дома», получают все большее распространение. Ими оборудуются не только дома и коттеджи, но и государственные учреждения, стадионы, бизнес-центры, отели, рестораны, аэропорты и т. д. Системы «умного дома» становятся все более функциональными, они позволяют автоматизировать процесс управления самыми различными параметрами системы жизнеобеспечения [1]. Растущая популярность таких систем в настоящее время объясняется широким набором функциональных возможностей, которые они предоставляют оператору. Однако чем более многофункциональными становятся системы автоматизированного управления зданиями, тем большей опасности они подвергаются со стороны мошенников [2].

На сегодняшний день системы «умного дома» не обладают полноценной защищенностью от компьютерных и иного рода атак злоумышленников. В связи с этим возникает опасность, что мошенник, используя уязвимости системы, сможет дистанционно управлять «умным домом» [3]. Например, он может целенаправленно выключить один из приборов или включить его в любое время, даже когда хозяина нет дома. Подобные манипуляции с электроприборами могут привести к возгоранию. Зачастую такими возможностями пользуются злоумышленники для того, чтобы запугать жертву или на время отключить освещение для проникновения в дом.

Данная статья посвящена исследованию возможных уязвимостей системы «умного дома», построенной на технологии X10.

Технология X10 является одной из самых распространенных технологий автоматизированного управления зданием, на которых основаны самые первые интеллектуальные здания. X10 определяет методы и протокол передачи сигналов управления электронными модулями, к которым подключены бытовые электроприборы, с использованием обычной электропроводки или беспроводных каналов.

В сети X10 все устройства можно разбить на две большие группы:

- контролеры;
- исполнительные модули.

Контролеры отвечают за генерацию команд X10 и передачу этих команд в сеть. Помимо ручного кнопочного управления контролеры могут иметь встроенный таймер или специализированное устройство ввода внешнего воздействия, как, например, датчик освещенности, фотоприемник инфракрасного излучения от пульта дистанционного управления и другие.

Исполнительный модуль, выполняя команды, передаваемые тем или иным контролером, управляет прибором, подключенным к системе автоматизированного управления зданием.

Также в состав сети X10 могут входить трансиверы, принимающие сигналы от инфракрасных или радиопультов дистанционного управления и передающие их в электросеть, преобразовав в формат X10.

Передача сигналов по сети идет посредством высокочастотных импульсов, с помощью которых кодируется цифровая информация [4]. Импульсы представляют собой пакеты переменного напряжения амплитудой 5 В, частотой 120 КГц и длительностью 1 мс, что определяет бинарную единицу (единичный бит); бинарный ноль — отсутствие импульса.

Передача импульсов синхронизирована с переходом переменного тока через нулевой уровень в пределах 200-микросекнудного интервала. Единичный бит передается в виде трех импульсов с

интервалом 3,33 мс (для сети с частотой напряжения 50 Гц), которые соответствуют нулям трех фаз трехфазной электрической сети.

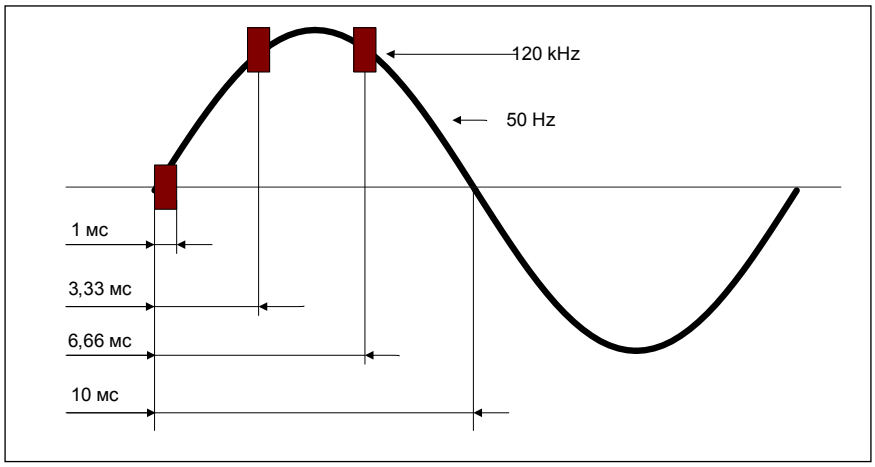

Рис. 1. Передача импульса по стандарту X10

Для передачи команды X10 требуется одиннадцать циклов (периодов) силового напряжения. Первые два цикла передают стартовый код. Этот код обозначает, что за ним последует команда. Следующие четыре цикла представляют код дома и последние пять циклов передают код прибора (с 1 по 16) или код функции («вкл», «выкл» и т. д.), т. е. ключевой код.

Когда сеть X10 установлена, каждый модуль сети настраивается таким образом, чтобы откликаться на один из 256 возможных адресов (16 кодов домов Ч 16 кодов модулей = 256). Каждый модуль реагирует только на команды, отправленные непосредственно ему, а также еще на несколько широковещательных команд.

Каждый полный код команды, который включает в себя стартовый код, код дома и ключевой код, всегда передается дважды непрерывным блоком. Между блоками разных команд всегда должен быть перерыв в три цикла силового напряжения. Исключением из этого правила являются блоки команд «ярче»/«темнее», которые передаются последовательно (минимум два блока) без задержек.

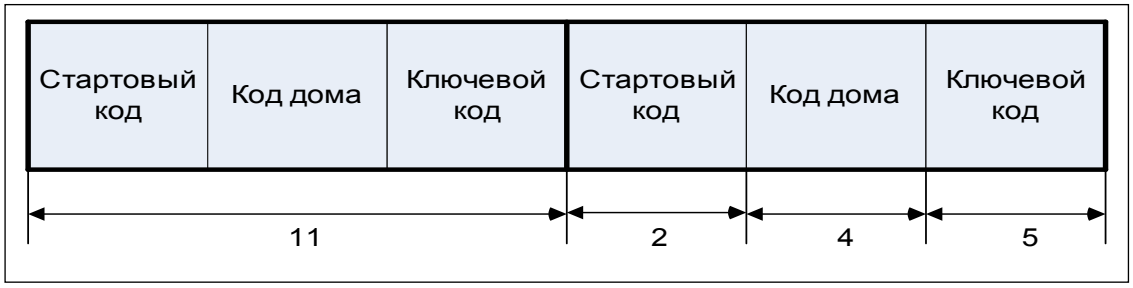

Рис. 2. Формат передачи полного кода

Внутри каждого блока код дома и ключевой код должны передаваться с дополняющими до единицы кодами в смежных полупериодах силового напряжения. Например, если единичный импульс передан в первой половине периода, то во второй не должно быть никакого сигнала (нулевой бит).

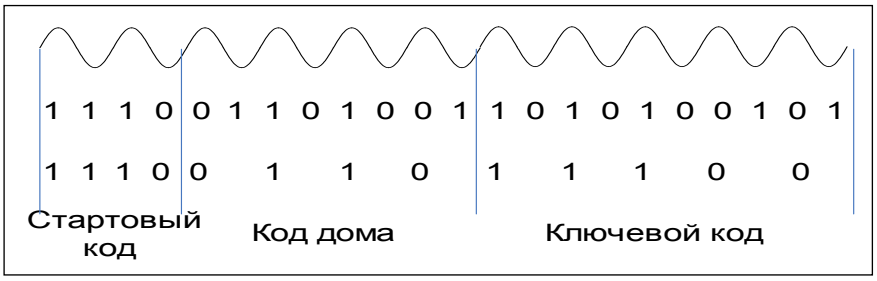

Рис. 3. Фактическая передача полного кода в электросети

Стартовый код — это уникальный код, всегда равный 1110 и не имеющий дополняющих бит в смежных полупериодах, т. е. значащие биты передаются на каждый переход силового напряжения через нуль.

Таблица 1 показывает возможные значения кода дома и ключевого кода и их двоичные представления.

Таблица 1. Двоичные представления кодов для формирования датаграмм

Коды домов						**Ключевые коды**				
	H1	**H2**	**H4**	**H8**		**D1**	**D2**	**D4**	**D8**	**D16**
A	0	1	1	0	**1**	0	1	1	0	0
B	1	1	1	0	**2**	1	1	1	0	0
C	0	0	1	0	**3**	0	0	1	0	0
D	1	0	1	0	**4**	1	0	1	0	0
E	0	0	0	1	**5**	0	0	0	1	0
F	1	0	0	1	**6**	1	0	0	1	0
G	0	1	0	1	**7**	0	1	0	1	0
H	1	1	0	1	**8**	1	1	0	1	0
I	0	1	1	1	**9**	0	1	1	1	0
J	1	1	1	1	**10**	1	1	1	1	0
K	0	0	1	1	**11**	0	0	1	1	0
L	1	0	1	1	**12**	1	0	1	1	0
M	0	0	0	0	**13**	0	0	0	0	0
N	1	0	0	0	**14**	1	0	0	0	0
O	0	1	0	0	**15**	0	1	0	0	0
P	1	1	0	0	**16**	1	1	0	0	0
Все модули «Выкл»						0	0	0	0	1
Весь свет «Вкл»						0	0	0	1	1
«Вкл»						0	0	1	0	1
«Темнее»						0	0	1	1	1
«Ярче»						0	1	0	1	1
Весь свет «Выкл»						0	1	1	0	1
Дополнительный код						0	1	1	1	1

HAIL запрос	0	0	0	0	1
HAIL ответ	1	0	0	1	1
Предустановка диммера	1	0	1	X	1
Дополнительные данные	1	1	0	0	1
Статус «Вкл»	1	1	0	1	1
Статус «Выкл»	1	1	1	0	1
Запрос статуса	1	1	1	1	1

К примеру, чтобы включить пятый модуль в «доме К», нужно отправить по электросети следующую строку бит:

1110010110100101011001111001011010010101100100000011100101101001011001101110010110100101100110

Эта датаграмма содержит 94 бита и займет 47 циклов силового напряжения, или 0,94. Поэтому при нажатии на кнопку «вкл» свет включается с запаздыванием. Реакция на команды «Весь свет "вкл"» или «Все модули "выкл"» заметно быстрее, так как не передается код модуля.

Кажущаяся надежность системы X10, тем не менее, уязвима. Дело в том, что если в двух соседних квартирах, использующих одну и ту же фазу осветительной сети, применяются устройства X10, то существует возможность несанкционированной передачи управляющих сигналов X10 из одной квартиры через электрическую сеть в другую квартиру.

К сожалению, при проектировании большинства систем автоматизированного управления зданием вопросу несанкционированного доступа к устройствам из электрической сети практически никто не придает особого значения. Осуществить атаку на объект, оборудованный приборами X10, не составляет большого труда. Достаточно запрограммировать необходимым образом несанкционированно подключенный к сети прибор, способный передавать датаграммы в формате X10.

Самая простая атака отключения света на интересующем злоумышленника объекте будет заключаться в отправке в сеть всего лишь одной датаграммы следующего формата:

1110011010010101010110111001101001010101010110

Эта датаграмма говорит о том, что все устройства в сети X10 должны получить сигнал о немедленном отключении.

Чтобы отправить такую датаграмму в сеть, достаточно подключить к электросети специальный переходник, который, в свою очередь, по USB-проводу подключается к компьютеру. Это позволяет передавать в сеть управляющие команды, используя специальное программное обеспечение.

Но это не единственная возможность для злоумышленника атаковать систему «умного дома», построенную на протоколе X10. Другой вариант — это использование радиоканала управления. Такой способ атаки позволяет осуществлять несанкционированное управление сетью при отсутствии возможности несанкционированного подключения к силовой проводке. Уязвимость в радиоканале также заключается в том, что протокол X10 не предусматривает никакой системы паролей и предполагает совместимость любого передатчика управляющих сигналов с любым приемником (исполнительным устройством). Наличие системы паролирования заметно усложнило бы устройства X10.

Таким образом, технически возможен умышленный несанкционированный доступ по радиоканалу к устройствам X10. Диапазоны частот 310 МГц и 433 МГц, применяемые в радиоканалах X10, широко используются в системах охранно-пожарных сигнализаций, в автомобильных сигнализациях и т. п.

Рабочие частоты передатчика и приемника не стабилизированы и определяются настройкой LC-контуров. Это облегчает достижение совместимости любого передатчика управляющих

сигналов с любым приемником. Одновременно с этим облегчается и задача злоумышленника — нет необходимости в точном подборе частоты передатчика, применяемого для атаки.

Возможны как минимум два варианта атаки на устройства X10 посредством радиоканала. Во-первых, это подача извне здания нежелательных команд управления. Во-вторых, это передача извне радиочастотных помех, препятствующих правильной работе радиоканала X10 между передатчиками управляющих сигналов и приемниками. Хотя для этого нужна довольно высокая мощность передатчика, создающего помехи, но технически это реализуемо. С точки зрения хозяев дома, результат атаки будет выглядеть как потеря управляемости исполнительными устройствами X10.

Описанный сценарий атаки на сеть X10 с несанкционированным доступом в систему автоматизированного управления зданием можно предотвратить при соблюдении следующих мер предосторожности.

Так как управляющие сигналы в сети X10 передаются по электрической сети на частоте около 120 кГц, отличающейся от основной частоты сети (50 Гц) на три порядка, то посредством фильтрации они могут быть легко подавлены. Такая фильтрация выполняется штатными устройствами X10 — фильтрами типа FD10. Такой фильтр устанавливается на вводе электрической сети в жилое помещение. Поскольку атака через электросеть с физической точки зрения эквивалентна созданию взаимных помех между соседними квартирами, то FD10 полностью решит вопрос отражения подобной атаки.

Таким образом, для пресечения атак на систему X10 необходимо на этапе проектирования заложить фильтр FD10 как необходимое условие безопасности.

Если говорить о защите от радиоатак на системы автоматизированного управления зданием, построенных на основе технологии X10, то одним из вариантов защиты является введение паролей на соединяемые по радиоканалу устройства.

В современных условиях добавление паролей к передаваемым управляющим сигналам X10 — вполне посильная задача для микропроцессорной техники (например, по аналогии с динамическими кодами, применяемыми в автомобильных сигнализациях). Именно такой механизм реализуется во многих модулях для системы.

Снизить вероятность атаки по радиоканалу можно за счет уменьшения эффективной чувствительности радиоприемника X10 (например, путем расположения его как можно дальше от периметра территории здания). Кроме того, если потенциальная угроза атаки по радиоканалу рассматривается как неприемлемая, то можно отказаться от радиопультов и использовать только инфракрасные пульты управления.

СПИСОК ЛИТЕРАТУРЫ:

1. *Кусакин И. И.* Программно-аппаратный комплекс автоматизированного контроля целостности инфраструктуры жилых помещений для социального обеспечения // XV Международная телекоммуникационная конференция молодых ученых и студентов «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3-х частях. Ч. 3. М.: НИЯУ МИФИ, 2012. С. 156–157.

2. *Смирной А. С., Стариковский А. В.* Система автоматического удаленного считывания и передачи показателей со счетчиков в жилых комплексах // XIV Международная телекоммуникационная конференция молодых ученых и студентов «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3-х частях. Ч. 3. М.: НИЯУ МИФИ, 2011. С. 188–189.

3. *Аристов М. С.* Антивирусный программно-аппаратный комплекс для систем автоматизированного здания // XIV Международная телекоммуникационная конференция молодых ученых и студентов «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3-х частях. Ч. 3. М.: НИЯУ МИФИ, 2011. С. 151–152.

4. Феноменальный источник ресурсов сети. Кодирование информации в локальных сетях. URL: http://firs.ucoz.com/index/kodirovanie_informacii_v_lokalnykh_setjakh/0-232.