§7 МОДЕЛИ И МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Иванов С.Е., Хлопотов М.В., Иванова Л.Н.

ПОСТРОЕНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОФИСА НА ОСНОВЕ СЕТИ Z-WAVE

Аннотация: *Предметом исследования является комплексная система обеспечения безопасности офиса на основе сетей Z-Wave. Проектируется комплексная система для контроля офиса на основе сети Z-Wave с возможностью мобильного управления. Безопасность офиса основывается на комплексной системе контроля и управления оборудованием, устройствами, датчиками состояния, пожарной сигнализацией. Проектируемая комплексная система безопасности объединяет управление и контроль над важнейшими офисными объектами: статус датчиков пожарной сигнализации, состояние основных электрических устройств и статус механизмов замков дверей и окон. Представлены разработанные на JavaScript функции, посредством которых выполняется контроль и управление системой безопасности офиса. Предложен метод управления комплексной системой безопасности посредством мобильного устройства с операционной системой Android. Приводятся основные команды для управления устройствами в сети Z-Wave. Разработанный комплекс обеспечения безопасности для офисов существенно увеличивает уровень безопасности и позволяет непрерывно контролировать необходимые устройства через мобильное приложение. Приведены технология, метод и необходимое оборудование для построения комплексной системой безопасности офиса. Невысокая стоимость построения комплекса безопасности позволяет широко применять его во всех сферах бизнеса.*

Ключевые слова: *сети Z-Wave, система безопасности, радио-протокол Z-Wave, офисное оборудование, управление, Android, датчики, мобильное устройство, мобильное приложение, контроллеры*

Abstract: *The subject of this study is a comprehensive office security system based on Z-Wave network. The authors design a comprehensive system for office monitoring based on the Z-Wave network with mobile control feature. Office security is based on a comprehensive system of*

DOI: 10.7256/2305-6061.2016.4.21460

monitoring and controlling equipment, devices, condition sensors, fire alarm. The designed integrated security system includes the management and control of the major office facilities: the status of the fire alarm sensors, state of basic electrical devices and the status of the mechanisms of locks of doors and windows. The authors present JavaScript-based functions for running the control and management of the office security system. A method of managing complex security system through the mobile device with the Android operating system is suggested. The paper contains basic commands to control devices in the Z-Wave network. The designed complex security system significantly increases the level of security and allows to continuously monitor the appropriate device via the mobile app. The authors show technologies and the equipment necessary for the construction of an office complex security system. Low cost of building this security system allows to widely use it in all areas of business.

Keywords:*controllers, mobile app, mobile device, sensors, Android, control, office equipment, Z-Wave radio protocol, security system, Z-Wave network*

Введение

В современном офисном мире необходимо полностью контролировать устройства, оборудование и датчики без перерывов и пауз. Для этих целей проектируется комплексная система офисной безопасности. Проектируется комплексная система для контроля офиса на основе сети Z-Wave [1] с возможностью мобильного управления [2]. Управление комплексной системой безопасности осуществляется посредством мобильного устройства с операционной системой Android. В отличие от других систем безопасности, для которых необходимо обучение специалистов [3], разработанный комплекс не требует специальной подготовки. Разграничение полномочий управления над системой осуществляется с помощью авторизации пользователя по паролю.

Для построения систем обеспечения безопасности применимы различные технологии и методики [4]. Разработанный комплекс обеспечения безопасности включает в себя современные технологии Z-Wave, OpenRemote, RaZberry. Для управления устройствами предложено использовать реле, датчики и сенсоры с поддержкой сети Z-Wave. С помощью технологий сети Z-Wave можно поддерживать сотни устройств и управлять освещением, шторами, воротами, включением, выключением устройств, управлять обогревом, кондиционерами, детектировать события, получать данные со счетчиков и взаимодействовать с ПК через контроллер. Использование комплекса не требует применения специального правового обеспечения [5].

В отличие от аналогичных систем обеспечения безопасности [6-10] проектируемый комплекс выполнен с учетом оптимизации стоимости устройств и затрат на обслуживание. Невысокая стоимость построения комплекса безопасности позволяет широко применять его во всех сферах малого бизнеса. Применение комплекса для офисов существенно увеличивает уровень безопасности. Рассмотрение правовых аспектов безопасности [11-14] в работе представляется нецелесообразным, вследствие отсутствия защищенных пер-

DOI: 10.7256/2305-6061.2016.4.21460

сональных, коммерческих, закрытых данных и необходимости сертификации комплекса.

Радио-протокол сети Z-Wave позволяет передавать данные со скоростью до 100 Кбит/с. Для сети Z-Wave в Европе и России применяется частота 868 МГц. При создании гетерогенных сетей применим протокол сети Z-Wave, который обеспечивает совместимость устройств разных производителей. По сравнению с применяемым радио-протоколом Z-Wave аналогичный протокол ZigBee для сбора данных со счётчиков сложно совместим с устройствами разных производителей. Радио-протокол Z-Wave позволяет передавать данные между устройствами вне прямой видимости. Другим преимуществом использования протокола Z-Wave является гарантия доставки и повторная отправка, если пересылаемый пакет не был доставлен до получателя. Для аналогичного Z-Wave радио-протокола - EnOcean отсутствует подтверждения доставки пакета.

Сети Z-Wave находят свое широкое применение во многих областях автоматизации и управления различными механизмами и устройствами. В сети Z-Wave основной мастер контроллер управляет всеми узлами. Для сети Z-Wave назначен уникальный идентификатор HomeID, для каждого узла в сети назначен свой уникальный NodeID. Для защиты передачи данных в сети Z-Wave применяются короткие сеансы и шифрование AES с одноразовым ключом 128 бит. Шифрование в сети Z-Wave применяется в оконных системах, дверных замках и ПК контроллерах. Для управления устройствами сети Z-Wave применим интерфейс HTTP/JSON API.

Построение системы обеспечения безопасности с мобильным управлением

Разработанная комплексная система безопасности объединяет управление и контроль над важнейшими офисными объектами: статус датчиков пожарной сигнализации, состояние основных электрических устройств и статус механизмов замков дверей и окон. Например, посредством мобильного приложения можно управлять включением-выключением освещения в комнатах офиса, управлять кондиционером, контролировать статус датчиков противопожарной сигнализации, определять состояние открыто-закрыто для окон и дверей офиса.

Для реализации комплекса возможно использовать оборудование: реле Fibaro Single Switch, датчики открытия-закрытия Fibaro Door/Window Sensor

Для контроля устройств в сети Z-Wave посредством web применен интерфейс HTTP/JavaScript API. Ниже приведем разработанные на JavaScript функции, которые можно выполнить, послав HTTP запрос.

Функция JavaScript для включения устройства номер n имеет следующий вид:

```
switchon = function(n,i)
{ zway.devices[n].instances[i].switchbinary.set(255);}
```

Функция JavaScript для выключения устройства представлена в виде:

```
switchoff = function(n,i)
{ zway.devices[n].instances[i].switchbinary.set(0); }
```


DOI: 10.7256/2305-6061.2016.4.21460

Функция JavaScript для получения данных с сенсора имеет следующий вид:

```
sensorstatus = function(n,i)
{ return zway.devices[n].instances[i].sensorbinary.data.level.value; }
```

Функция JavaScript для запроса статуса устройства имеет вид:

```
switchstatus = function(n,i)
{ return zway.devices[n].instances[i].switchbinary.data.level.value; }
```

Здесь параметр n - номер устройства в сети, параметр i - номер канала внутри устройств.

Для вызова JavaScript включения устройства номер 1 необходимо выполнить HTTP запрос:

http://192.168.0.1:8081/js/run/switchon(1,1)

Для вызова JavaScript выключения устройства номер 1 необходимо выполнить HTTP запрос:

http://192.168.0.1:8081/js/run/switchoff(1,1)

Для вызова JavaScript получения данных с сенсора номер 2 необходимо выполнить HTTP запрос:

http://192.168.0.1:8081/js/run/sensorstatus(2,1)

Для вызова JavaScript получения статуса устройства номер 3 необходимо выполнить HTTP запрос:

http://192.168.0.1:8081/js/run/switchstatus(3,1)

Например, для получения информации о том включен или выключен свет, мы выполняем HTTP запрос для устройства номер 4:

http://192.168.0.1:8081/js/run/switchstatus(4,1)

Для включения и выключения света мы выполняем соответствующие HTTP запросы:

http://192.168.0.1:8081/js/run/switchon(4,1)

http://192.168.0.1:8081/js/run/switchoff(4,1)

Для получения информации о том закрыто ли окно, мы выполняем HTTP запрос для соответствующего сенсора номер 5:

http://192.168.0.1:8081/js/run/sensorstatus(5,1)

Устройствами в сети Z-Wave можно управлять посредством интерфейса HTTP/JSON API. Ниже приведены базовые команды для управления устройствами.

Для включения устройства номер 1 необходимо установить значение флага в 255 с помощью команды:

http://192.168.0.1:8081/zwaveapi/run/devices[1].instances[1].switchbinary.set(255)

Для выключения устройства номер 1 необходимо установить значение флага в 0 с помощью команды:

http://192.168.0.1:8081/zwaveapi/run/devices[1].instances[1].switchbinary.set(0)

DOI: 10.7256/2305-6061.2016.4.21460

Для получения данных с сенсора номер 2 (сработал - не сработал) нужно выполнить команду:

http://192.168.0.1:8081/zwaveapi/run/devices[2].instances[1]. sensorbinary.data.level.value;

Для получения состояния устройства номер 3 нужно выполнить команду:

http://192.168.0.1:8081/zwaveapi/run/devices[3].instances[1]. switchbinary.data.level.value;

Для управления устройствами в сети Z-Wave можно использовать плату RaZberry. С помощью контроллера RaZberry возможно объединить все устройства в единую систему.

Для разработки графического интерфейса и мобильного приложения мы применили облачный конструктор OpenRemote. Сервер OpenRemote получает команды от мобильного приложения и далее транслирует их контроллеру сети Z-Wave. После загрузки созданного в конструкторе приложения на контроллер OpenRemote его можно использовать в мобильном устройстве с операционной системой Android.

При внедрении данного комплекса возрастает уровень обеспечения безопасности офиса. При этом затраты на обслуживание и контролирование офиса для бизнеса не увеличиваются.

Заключение

Безопасность офиса основывается на комплексной системе контроля и управления оборудованием, устройствами, датчиками состояния, пожарной сигнализацией. Проектируется комплексная система для контроля офиса на основе сети Z-Wave с возможностью мобильного управления. Проектируемая комплексная система безопасности объединяет управление и контроль над важнейшими офисными объектами: статусом датчиков пожарной сигнализации, состоянием основных электрических устройств и статусом механизмов замков дверей и окон.

Управление комплексной системой безопасности может осуществляться с мобильного устройства с операционной системой Android. Приводятся основные команды для управления устройствами в сети Z-Wave. Следует отметить невысокую стоимость построения комплекса безопасности, которая открывает возможность широкого использования во всех сферах бизнеса. Применение комплекса для офисов существенно увеличивает уровень безопасности.

Библиография :

1. Hall, J., Ramsey, B., Rice, M., Lacey, T., Z-wave network reconnaissance and transceiver fingerprinting using software-defined radios, (2016) Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, pp. 163-171.

DOI: 10.7256/2305-6061.2016.4.21460

2. Wei, C.-C., Chen, Y.-M., Chang, C.-C., Yu, C.-H., The Implementation of Smart Electronic Locking System Based on Z-Wave and Internet, (2015) Proceedings-2015 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2015, art. no. 7379483, pp. 2015-2017.
3. Гузий А.Г., Лушкин А.М. Методические особенности подготовки специалистов по управлению безопасностью авиационных полетов // Вопросы безопасности. - 2016. - 3. - С. 30 - 40. DOI: 10.7256/2409-7543.2016.3.19013. URL: http://www.e-notabene.ru/nb/article_19013.html
4. Болкунов О.Н. Количественное измерение международной энергетической безопасности // Национальная безопасность / nota bene. - 2013. - 4. - С. 536 - 548. DOI: 10.7256/2073-8560.2013.4.8897.
5. Опалев А.В. Правовое обеспечение национальной безопасности: объект, предмет и задачи // Национальная безопасность / nota bene. - 2014. - 2. - С. 244 - 250. DOI: 10.7256/2073-8560.2014.2.11295.
6. Коробейников А.Г., Гришенцев А.Ю., Святкина М.Н. Применение интеллектуальных агентов магнитных измерений для мониторинга объектов железнодорожной инфраструктуры // Кибернетика и программирование. - 2013. - 3. - С. 9 - 20. DOI: 10.7256/2306-4196.2013.3.8737. URL: http://www.e-notabene.ru/kp/article_8737.html
7. Калюжный Ю.Н. Теоретико-правовые подходы к определению принципов обеспечения безопасности дорожного движения в Российской Федерации // Административное и муниципальное право. - 2016. - 11. - С. 902 - 909. DOI: 10.7256/1999-2807.2016.11.19506.
8. Серёгин С.Ф., Харитонов В.В. Ключевые проблемы совершенствования системы безопасности полетов государственной авиации // Транспортный вестник. - 2016. - 1. - С. 1 - 22. DOI: 10.7256/2453-8906.2016.1.19459. URL: http://www.e-notabene.ru/transport/article_19459.html
9. Кузнецова Е.И. Разработка инструментария обеспечения экономической безопасности предприятия // Национальная безопасность / nota bene. - 2015. - 1. - С. 101 - 107. DOI: 10.7256/2073-8560.2015.1.14317.
10. Куракин А.В., Кулешов Г.Н., Несмелов П.В. Информационная безопасность в системе государственной службы // Административное и муниципальное право. - 2013. - 2. - С. 172 - 176. DOI: 10.7256/1999-2807.2013.02.13.
11. И. С. Садикова Правовые аспекты защиты персональных данных // Право и политика. - 2012. - 4. - С. 758 - 761.
12. Р. М. Асланов, А. А. Морозов Системный анализ правового обеспечения информационной безопасности в Российской Федерации // Национальная безопасность / nota bene. - 2012. - 2. - С. 56 - 59.
13. Владимирова Т.В. Новые социальные мобильности как практики обеспечения информационной безопасности // Политика и Общество. - 2014. - 8. - С. 902 - 909. DOI: 10.7256/1812-8696.2014.8.11110.
14. Костенников М.В., Куракин А.В., Кулешов Г.Н., Несмелов П.В. Государственная служба и информационные технологии // Административное и муниципальное право. - 2012. - 12. - С. 27 - 34.

References:

1. Hall, J., Ramsey, B., Rice, M., Lacey, T., Z-wave network reconnaissance and transceiver fingerprinting using software-defined radios, (2016) Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, pp. 163-171.

DOI: 10.7256/2305-6061.2016.4.21460

2. Wei, C.-C., Chen, Y.-M., Chang, C.-C., Yu, C.-H., The Implementation of Smart Electronic Locking System Based on Z-Wave and Internet, (2015) Proceedings-2015 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2015, art. no. 7379483, pp. 2015-2017.
3. Guzii A.G., Lushkin A.M. Metodicheskie osobennosti podgotovki spetsialistov po upravleniyu bezopasnost'yu aviatsionnykh poletov // Voprosy bezopasnosti. - 2016. - 3. - C. 30 - 40. DOI: 10.7256/2409-7543.2016.3.19013. URL: http://www.e-notabene.ru/nb/article_19013.html
4. Bolkunov O.N. Kolichestvennoe izmerenie mezhdunarodnoi energeticheskoi bezopasnosti // Natsional'naya bezopasnost' / nota bene. - 2013. - 4. - C. 536 - 548. DOI: 10.7256/2073-8560.2013.4.8897.
5. Opalev A.V. Pravovoe obespechenie natsional'noi bezopasnosti: ob"ekt, predmet i zadachi // Natsional'naya bezopasnost' / nota bene. - 2014. - 2. - C. 244 - 250. DOI: 10.7256/2073-8560.2014.2.11295.
6. Korobeinikov A.G., Grishentsev A.Yu., Svyatkina M.N. Primenenie intellektual'nykh agentov magnitnykh izmerenii dlya monitoringa ob"ektov zheleznodorozhnoi infrastruktury // Kibernetika i programmirovanie. - 2013. - 3. - C. 9 - 20. DOI: 10.7256/2306-4196.2013.3.8737. URL: http://www.e-notabene.ru/kp/article_8737.html
7. Kalyuzhnyi Yu.N. Teoretiko-pravovye podkhody k opredeleniyu printsipov obespecheniya bezopasnosti dorozhnogo dvizheniya v Rossiiskoi Federatsii // Administrativnoe i munitsipal'noe pravo. - 2016. - 11. - C. 902 - 909. DOI: 10.7256/1999-2807.2016.11.19506.
8. Seregin S.F., Kharitonov V.V. Klyuchevye problemy sovershenstvovaniya sistemy bezopasnosti poletov gosudarstvennoi aviatsii // Transportnyi vestnik. - 2016. - 1. - C. 1 - 22. DOI: 10.7256/2453-8906.2016.1.19459. URL: http://www.e-notabene.ru/transport/article_19459.html
9. Kuznetsova E.I. Razrabotka instrumentariya obespecheniya ekonomicheskoi bezopasnosti predpriyatiya // Natsional'naya bezopasnost' / nota bene. - 2015. - 1. - C. 101 - 107. DOI: 10.7256/2073-8560.2015.1.14317.
10. Kurakin A.V., Kuleshov G.N., Nesmelov P.V. Informatsionnaya bezopasnost' v sisteme gosudarstvennoi sluzhby // Administrativnoe i munitsipal'noe pravo. - 2013. - 2. - C. 172 - 176. DOI: 10.7256/1999-2807.2013.02.13.
11. I. S. Sadikova Pravovye aspekty zashchity personal'nykh dannykh // Pravo i politika. - 2012. - 4. - C. 758 - 761.
12. R. M. Aslanov, A. A. Morozov Sistemnyi analiz pravovogo obespecheniya informatsionnoi bezopasnosti v Rossiiskoi Federatsii // Natsional'naya bezopasnost' / nota bene. - 2012. - 2. - C. 56 - 59.
13. Vladimirova T.V. Novye sotsial'nye mobil'nosti kak praktiki obespecheniya informatsionnoi bezopasnosti // Politika i Obshchestvo. - 2014. - 8. - C. 902 - 909. DOI: 10.7256/1812-8696.2014.8.11110.
14. Kostennikov M.V., Kurakin A.V., Kuleshov G.N., Nesmelov P.V. Gosudarstvennaya sluzhba i informatsionnye tekhnologii // Administrativnoe i munitsipal'noe pravo. - 2012. - 12. - C. 27 - 34.