http://vestnik.mrsu.ru

ISSN Print 0236-2910
ISSN Online 2313-0636

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ / COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 004.738.5’056 DOI: 10.15507/0236-2910.028.201801.085-094

Анализ угроз информационной безопасности протоколов и систем управления освещением

С. Н. Ивлиев*, С. Л. Крылова, С. А. Шиков
ФГБОУ ВО «МГУ им. Н. П. Огарёва» (г. Саранск, Россия)
**ivliev_sn@mail.ru*

Введение. В статье рассматриваются возможные угрозы в сфере информационной безопасности при использовании PLC-технологий (power line communications). Подобные технические решения дают возможность управления и обратной связи с управляемыми устройствами, однако данные технологии не соответствуют необходимому уровню информационной безопасности. В статье предлагаются пути решения данной проблемы.
Материалы и методы. Рассмотрены объекты и методы исследования; указаны проводимые исследования и список решаемых задач, проведен анализ угроз информационной безопасности.
Результаты исследования. Приводится общая модель информационной системы, а также модель угроз для системы управления освещением по протоколу Dali.
Обсуждение и заключения. Были сделаны выводы по уязвимостям рассмотренных примеров. Даны общие рекомендации о необходимых действиях по увеличению уровня безопасности в сегменте протоколов управления освещением. Был составлен список минимальных объемов мероприятий по обеспечению безопасного функционирования систем освещения: идентификация и аутентификация субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защита машинных носителей информации; регистрация событий безопасности; антивирусная защита; обнаружение вторжений и др.

Ключевые слова: информационная безопасность, угроза информационной безопасности, информационная система, управление освещением, PLC-технологии

Для цитирования: Ивлиев С. Н., Крылова С. Л., Шиков С. А. Анализ угроз информационной безопасности протоколов и систем управления освещением // Вестник Мордовского университета. 2017. Т. 27, № 4. С. 85–94. DOI: 10.15507/0236-2910.028.201801.085-094

The Analysis of Threats to Information Security of Protocols and Lighting Control Systems

S. N. Ivliyev*, S. L. Krylova, S. A. Shikov
National Research Mordovia State University (Saransk, Russia)
**ivliev_sn@mail.ru*

Introduction. The paper considers the possible threats to information security when using PLC-technologies (power lines). Such technical solutions allow controlling and providing feedback with controllable devices. However, these technologies do not meet the safety requirements. The purpose of this investigation is to explore the problem and suggest solutions.
Materials and Methods. The aims and methods of investigation are presented. The conducted researches and the list of solved problems are indicated. The analysis of information security threats has been carried out.
Results. The study presents a general information system model. The model of threats to the lighting control system was developed using the Dali protocol.
Discussion and Conclusions. The authors have analyzed the factors that determine vulnerabilities of the analyzed examples. The level of safety in the segment of lighting control protocols must be increased. We provide the list of minimum measures to ensure the safe operation of lighting systems. The findings of this study have a number of important implications for future practice.

Keywords: information security, information security threat, information system, lighting control, PLC-technologies

For citation: Ivliyev S. N., Krylova S. L., Shikov S. A. The Analysis of Threats to Information Security of Protocols and Lighting Control Systems. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2018; 28(1):85–94. DOI: 10.15507/0236-2910.028.201801.085-094

Введение

Одним из наиболее современных направлений в области энергосбережения и энергоэффективности является внедрение систем интеллектуального управления. Наиболее эффективным решением принято считать применение PLC-технологий (power line communications), или управление оконечными устройствами энергопотребления по сетям электропитания. Используемые в практике технические решения позволяют не только управлять потоками энергии, но и осуществлять «обратную связь» с целью контроля эксплуатационных параметров управляемой системы. По аналогичной схеме построен и т. н. «интернет вещей». Даже имеются решения по передаче данных для ограниченного круга потребителей в условиях «последней мили». На рынке присутствует большое количество предложений управляющих контроллеров и модемов для подключения информационных каналов к сетям электроснабжения. При этом большинство технических решений использует фирменные технологии и совершенно не учитывает аспекты информационной безопасности. Исследованию указанной проблемы и посвящена данная работа.

Обзор литературы

Имеется огромное количество научного материала, касающегося технических аспектов использования указанных технологий, например, порядка подключения контроллеров или модемов [1–3]. При этом основное внимание уделяется вопросам электромагнитной совместимости и передаточных характеристик каналов связи, использующих линии электропередач [4–6]. Ограниченное количество исследований

посвящено изучению технических каналов утечки информации в PLC-системах [7–9].

Интересным представляется материал по изучению возможностей применения PLC-технологий Yitran в системе управления блокировками безопасности распределительных устройств высокого напряжения [6]. В данной работе предлагается оценивать надежность передачи информации на основании спектрального анализа сигнала, при этом отмечается зависимость характеристик передачи сигнала от параметров потребителей электроэнергии.

На основании изученного материала можно сделать вывод о многокомпонентности системы управления освещением. При таком подходе значительно увеличивается количество актуальных угроз, связанных с перехватом управления объектом. На базе Института электроники и светотехники ФГБОУ ВО «МГУ им. Н. П. Огарёва» также рассматривались вопросы безопасности информационных систем, предназначенных для управления технологическим оборудованием и построенных по принципу «Интернета вещей»[1–2] [10].

В связи с этим представляется необходимым исследовать надежность протоколов управления системами освещения. На основе анализа предложений по решению вопросов удаленного управления системами освещения констатируем, что наиболее распространенными протоколами управления системами освещения являются промышленные протоколы 1-10В, DMX, Dali. Первый из отмеченных протоколов является аналоговым, и его использование ограничивается небольшими осветительными установками, в основном при бытовом освещении.

Протоколы DMX и Dali позволяют управлять осветительными установками, где объекты управления могут располагаться на удалении от систем управления на расстоянии от нескольких сотен метров до нескольких километров. При этом протокол Dali является открытым и поддерживается такими крупными производителями осветительной арматуры как OSRAM. Необходимо отметить, что эти протоколы, как указано в спецификации, не являются протоколами безопасной передачи данных и требуют применения дополнительных средств обеспечения защиты информации[3–6].

Материалы и методы

Целью представленной работы является выработка рекомендаций по построению систем управления осве-

[1] **Ивлиев С. Н.** Интернет вещей: новые угрозы информационной безопасности // Проблемы и перспективы развития отечественной светотехники, электротехники и энергетики : мат-лы XII Всерос. науч.-техн. конф. с междунар. участием (г. Саранск, 28–29 мая 2015 г.) в рамках III Всерос. светотехнич. форума с междунар. участием. Саранск : Издатель Афанасьев В. С., 2015. С. 435–441. URL: https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-internet-veschey

[2] **Ивлиев С. Н.** Решение проблем безопасности информационно-технологического комплекса предприятий светотехнической отрасли на основе международных стандартов // Проблемы и перспективы развития отечественной светотехники, электротехники и энергетики : мат-лы XII Всерос. науч.-техн. конф. с междунар. участием (г. Саранск, 28–29 мая 2015 г.) в рамках III Всерос. светотехнич. форума с междунар. участием. Саранск : Издатель Афанасьев В. С., 2015. С. 428–434. URL: https://elibrary.ru/item.asp?id=24179114

[3] Руководство по применению DMX512. URL: http://dsl.msk.ru/rus/around/dmx512/ dmx512.htm

[4] OSRAM Professionals LMS DALI index. URL: http://www.osram.ru/osram_ru/Professionals/LMS/DALI_/index.htm

[5] OSRAM Professionals ECG ECGs for FL and CFL Dimmable ECGs with DALI QTi DALI DIM-CFL index. URL: http://www.osram.ru/osram_ru/Professionals/ECG/ECGs_for_FL_and_CFL/Dimmable_ECGs_with_DALI_/QTi_DALI_DIM-CFL/index.html

[6] OSRAM Professionals ECG ECGs for FL and CFL Dimmable ECGs with DALI QTi DALI DIM-T5 index. URL: http://www.osram.ru/osram_ru/Professionals/ECG/ECGs_for_FL_and_CFL/Dimmable_ECGs_with_DALI_/QTi_DALI_DIM-T5/index.html

щением с точки зрения обеспечения информационной безопасности. Для ее достижения были решены следующие задачи:

– проанализированы основные требования по безопасной эксплуатации промышленных программируемых контроллеров;

– изучены основные угрозы безопасности в автоматизированных системах управления технологическим оборудованием;

– выявлены актуальные угрозы безопасности;

– разработаны мероприятия по минимизации рисков, связанных с эксплуатацией систем управления освещением.

Основными нормативными документами, содержащими требования к программируемым контроллерам, является серия ГОСТ Р МЭК 61131[7], в частности, часть 6 «Безопасность функциональная». Для анализа угроз безопасности был использован банк угроз ФСТЭК России[8].

Требования по функциональной безопасности программируемых логических контроллеров (ПЛК-ФБ) в стандарте представлены в виде политик безопасности для всех этапов жизненного цикла изделия. Для обеспечения максимальной безопасности данных необходимо:

– логическое управление доступом к ПЛК-ФБ и между ними, включая человеко-машинные интерфейсы;

– административное управление, такое, чтобы для конкретного условия безопасности выполнялся общий подход по управлению и администрированию политики обеспечения безопасности на условиях единоначалия с общей ответственностью;

– физическое управление, ограничивающее несанкционированный доступ к ПЛК-ФБ (включая вспомогательные части, кабельные соединения, разъемы).

Общими угрозами в области информационной безопасности в системах автоматического управления на основании банка угроз ФСТЭК, являются:

– угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам (УБИ.092);

– угроза несогласованности правил доступа к большим данным (УБИ.097);

– угроза подмены беспроводного клиента или точки доступа (УБИ.126);

– угроза перехвата управления автоматизированной системой управления технологическими процессами (УБИ.183);

– угроза перехвата вводимой и выводимой на периферийные устройства информации (УБИ.115);

– угроза перехвата привилегированного потока (УБИ.117);

– угроза перехвата исключения/сигнала из привилегированного блока функций (УБИ.163);

– угроза перехвата одноразовых паролей в режиме реального времени (УБИ.181).

При актуализации угроз в системах управления освещением учитывалось, что основным элементом, обеспечивающим функционирование системы управления освещением, является телекоммуникационная сеть. Через данную сеть производится съем информации с различного рода датчиков и передача их главному контроллеру для обработки. Контроллер после обработки информации осуществляет передачу сигналов управления на исполнительные элементы. Через центральный контроллер происходит настройка и управление системой освещения легальным пользователем, а также через него при необходимости осуществляется передача

[7] ГОСТ Р МЭК 61131. URL: http://www.internet-law.ru/gosts/gost/61912

[8] Банк угроз информационной безопасности. URL: http://bdu.fstec.ru/threat?page=3

заданной информации пользователю системы через внешнюю сеть при его отсутствии в помещении (например, о несанкционированном проникновении). Такая телекоммуникационная сеть может быть построена с использованием как проводных, так и беспроводных каналов связи, например, Wi-Fi, Bluetooth или 3G.

Анализ угроз и нарушений безопасности необходимо проводить для связанных с безопасностью применений систем автоматического управления освещением с целью защиты как от преднамеренных атак, так и от неумышленных изменений параметров функционирования[9].

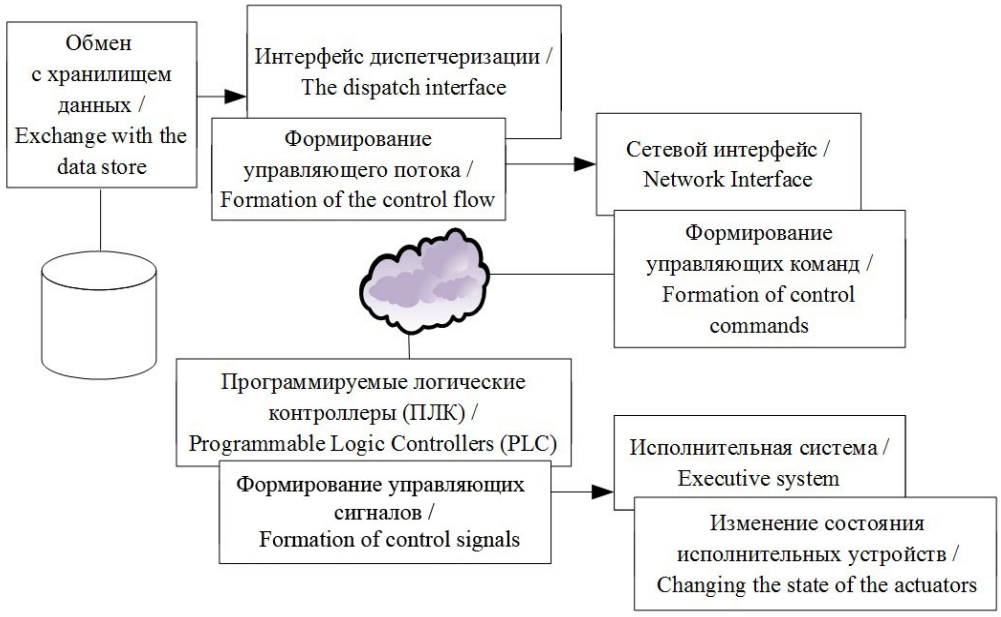
Безопасность может быть достигнута с помощью компенсирующих мер обеспечения безопасности и выполнения защитных мероприятий, таких как физические (например, механические средства, электронные средства) или организационные.

Если связанные с безопасностью коммуникации являются частью PLC-систем, то существует возможность непреднамеренных изменений параметров сетевых устройств. Связанные с безопасностью коммуникационные устройства должны иметь средства защиты от непреднамеренных изменений.

Результаты исследования

Для построения общей модели угроз системы управления освещением была построена общая модель информационной системы (рисунок).

При построении данной общей модели угроз особое внимание было уде-



Р и с у н о к. Общая модель информационной системы
F i g u r e. The general model of the information system

[9] Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». URL: http://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

лено уровню ПЛК, поскольку для исследуемой информационной системы этот уровень наиболее уязвим с точки зрения надежности протокола и, кроме того, нарушение свойств безопасности на этом уровне приводит к наиболее существенным нарушениям в работе управляемой системы.

На основании выше изложенного была построена модель угроз для системы управления освещением по протоколу Dali, представленная в таблице.

Таблица

Table

Модель угроз системы управления освещением

The model of threats to the lighting control system

Описание угрозы / Threat description	Содержание угрозы / Threat content	Источник / Source	Вероятность реализации угрозы / Probability of threat realization
1	*2*	*3*	*4*
Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам / Threat of unauthorized remote out-of-band access to hardware	Угроза обусловлена невозможностью контроля над механизмом, реализующего функции удаленного доступа на аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств, т. к. данный механизм предусматривает процедуру удаленного включения/выключения аппаратных устройств / The threat is caused by the inability to control the mechanism that implements the functions of remote access at the hardware level, at the level of the operating system, and independence from the state of power of the hardware devices. This mechanism provides a procedure for remote on/off of hardware devices	Внешний нарушитель с высоким потенциалом / External violator with high potential	Средняя / Medium
Угроза несогласованности правил доступа к большим данным / Threat of inconsistency of access rules to large data	Угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных / The threat is caused by the inadequacy of measures to differentiate and harmonize access to information from various users in a large data warehouse	Внутренний нарушитель с низким потенциалом / Internal intruder with low potential	Высокая, для систем наружного освещения объектов большой площади / High, for outdoor lighting systems of large areas
Угроза подмены беспроводного клиента или точки доступа / Threat of spoofing a wireless client or access point	Угроза обусловлена слабостями механизма аутентификации субъектов сетевого взаимодействия при беспроводном доступе / The threat is due to the weaknesses of the mechanism for authentication of subjects of network interaction with wireless access	Внешний нарушитель с низким потенциалом / External offender with low potential	Высокая, при наличии беспроводных сегментов сети / High, if there are wireless network segments

Продолжение табл. / Table continuation

1	*2*	*3*	*4*
Угроза перехвата управления автоматизированной системой управления технологическими процессами / Threat of interception of control by an automated process control system	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счет получения нарушителем права управления входящей в ее состав автоматизированной системой управления технологическими процессами путем эксплуатации уязвимостей ее программного обеспечения или слабостей технологических протоколов передачи данных / The threat lies in the ability of the violator to perform unauthorized access to the information infrastructure by getting the violator the right to manage the automated process control system included in its composition by exploiting the vulnerabilities of its software or the weaknesses of technological data transfer protocols	Внутренний нарушитель со средним потенциалом / Internal offender with medium potential	Высокая / High
		Внешний нарушитель с высоким потенциалом / External violator with high potential	Маловероятна / Unlikely
Угроза перехвата вводимой и выводимой на периферийные устройства информации / Threat of interception of information entered and output to peripheral devices	Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты, вводимой и выводимой на периферийные устройства информации с помощью криптографических средств / The given threat is caused by insufficiency of measures of protection of the information from leak and the control of data flows, and also impossibility of realization of protection of the information entered and deduced on peripheral devices by means of cryptographic means	Внутренний нарушитель с низким потенциалом / Internal intruder with low potential	Высокая / High
		External offender with low potential	Высокая / High
Угроза перехвата привилегированного потока / Threat of interception of privileged flow	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к потоку данных, созданного приложением с дополнительными привилегиями / The threat consists in the possibility of the violator making unauthorized access to the data stream created by the application with additional privileges	Внутренний нарушитель со средним потенциалом / Internal offender with medium potential	Маловероятна / Unlikely
		Внешний нарушитель со средним потенциалом / External offender with medium potential	Средняя / Medium

Окончание табл. / End of table

1	*2*	*3*	*4*
Угроза перехвата исключения/ сигнала из привилегированного блока функций / Threat of intercepting an exception/ signal from a privileged function block	Угроза заключается в возможности нарушителя получить права на доступ к защищаемой информации путем перехвата исключений/ сигналов, сгенерированных участком программного кода, исполняемого с повышенными привилегиями / The threat lies in the ability of the infringer to gain access to the protected information by intercepting exceptions/signals generated by a piece of code run with elevated privileges	Внутренний нарушитель со средним потенциалом / Internal offender with medium potential	Средняя / Medium
		Внешний нарушитель со средним потенциалом / External offender with medium potential	Маловероятна / Unlikely
Угроза перехвата одноразовых паролей в режиме реального времени / Threat of intercepting one-time passwords in real time	Угроза заключается в возможности получения нарушителем управления критическими операциями пользователя путем перехвата одноразовых паролей, высылаемых системой автоматически, и использования их для осуществления неправомерных действий до того, как истечет их срок действия (5–7 мин) / The threat consists in the possibility of the violator getting control over critical user operations by intercepting one-time passwords sent automatically by the system and using them to carry out illegal actions before their expiry date expires (5–7 minutes)	Внешний нарушитель со средним потенциалом / External offender with medium potential	Средняя / Medium

Обсуждение и заключения

На основании представленного анализа сделаем следующие выводы.

1. Для всех известных угроз безопасности существует значительная вероятность их реализации.

2. Для компенсации рисков, связанных с реализацией представленных угроз, необходимо использовать дополнительные мероприятия и технические решения.

3. При проектировании систем управления освещением необходимо дополнительно руководствоваться стандартами в области информационной безопасности.

Минимальный объем мероприятий по обеспечению безопасного функционирования систем освещения должен соответствовать требованиям регулятора[10] и содержать следующие комплексы мер:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации;

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение вторжений;

– контроль (анализ) защищенности информации;

– обеспечение целостности;

– обеспечение доступности;

– защита технических средств.

[9] URL: http://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. **Кузьминов К.** Реализация «умных» сетей на базе компонентов PLC от Texas Instruments // Новости электроники. 2013. № 7. URL: http://www.compel.ru/lib/ne/2013/7/7-realizatsiya-umnyih-setey-na-baze-komponentov-plc-ot-texas-instruments

2. **Девендран С., Мисра А., Мишра С.** Источник питания для беспроводного диммера без использования нейтрали: типовая разработка и ее испытания // Новости электроники. 2017. № 2. С. 33–43. URL: https://www.terraelectronica.ru/files/news/NE_02_2017_s33.pdf

3. **Кондратьев В.** Связь по электрическим сетям: принципы, стандарты, приложения // Электронные компоненты. 2011. № 12. С. 40–44. URL: http://ns1.russianelectronics.ru/leader-r/review/2327/doc/57948

4. **Зусев С. А.** Использование проводных и беспроводных интерфейсов на энергетических объектах, на примере PLC-систем и беспроводного интерфейса ZigBee // Современные научные исследования и инновации. 2016. № 4. URL: http://web.snauka.ru/issues/2016/04/67031

5. **Колокольникова А. И., Карнаухов Д. В.** Об автоматизированном контроле энергопотребления // Проблемы современной науки. 2013. № 8-1. С. 109–116. URL: https://elibrary.ru/item.asp?id=19144150

6. Применение PLC-технологий Yitran в системе управления блокировками безопасности распределительных устройств высокого напряжения / Р. К. Борисов [и др.] // Электричество. 2014. № 12. С. 18–23. URL: https://elibrary.ru/item.asp?id=22490944

7. **Балаев А. А., Горбатов В. С., Сепашвили Д. Т.** Тестирование безопасности PLC-технологии передачи данных // Безопасность информационных технологий. 2011. № 1. С. 57–60. URL: https://elibrary.ru/item.asp?id=18813084

8. **Балаев А. А., Горбатов В. С.** Методика аттестационных испытаний PLC-сетей на соответствие требованиям безопасности информации // Безопасность информационных технологий. 2012. № 1. С. 79–80. URL: https://elibrary.ru/item.asp?id=18811100

9. Методы обеспечения достоверности передачи информации в информационно-управляющих PLC-сетях предприятий / А. В. Щагин [и др.] // Информационные системы и технологии. 2014. Т. 83, № 3. С. 107–113. URL: http://elibrary.ru/item.asp?id=21574904

10. **Шиков С. А.** Проблемы информационной безопасности: интернет вещей // Вестник Мордовского университета. 2017. Т. 27, № 1. С. 27–40. DOI: 10.15507/0236-2910.027.201701.027-040

Поступила 19.10.2017; принята к публикации 20.12.2017; опубликована онлайн 20.03.2018

Об авторах:

Ивлиев Сергей Николаевич, заведующий кафедрой информационной безопасности и сервиса, Институт электроники и светотехники, ФГБОУ ВО «МГУ им. Н. П. Огарёва» (430005, Россия, г. Саранск, ул. Большевистская, д. 68), ResearcherID: E-1697-2014, ORCID: http://orcid.org/0000-0002-6101-3388, ivliev_sn@mail.ru

Крылова Светлана Львовна, старший преподаватель кафедры информационной безопасности и сервиса, Институт электроники и светотехники, ФГБОУ ВО «МГУ им. Н. П. Огарёва» (430005, Россия, г. Саранск, ул. Большевистская, д. 68), ResearcherID: L-7324-2017, ORCID: http://orcid.org/0000-0003-4083-9209, svet711@yandex.ru

Шиков Станислав Александрович, аспирант, преподаватель кафедры информационной безопасности и сервиса, Институт электроники и светотехники, ФГБОУ ВО «МГУ им. Н. П. Огарёва» (430005, Россия, г. Саранск, ул. Большевистская, д. 68), ResearcherID: S-2514-2016, ORCID: http://orcid.org/0000-0002-8412-5163, stenlav@mail.ru

Вклад соавторов:

С. Н. Ивлиев: научное руководство, разработка концепции модели угроз, анализ исходных данных; С. Л. Крылова: адаптация и актуализация модели угроз, построение адаптированной модели угроз с учетом требований регуляторов; С. А. Шиков: верстка статьи, подготовка графического материала, аналитическая обработка нормативной документации.

Все авторы прочитали и одобрили окончательный вариант рукописи.

REFERENCES

1. Kuzminov K. [Realization of “smart” networks based on PLC components from Texas Instruments]. *Novosti elektroniki* = Electronics News. 2013; 7. Available at: http://www.compel.ru/lib/ne/2013/7/7-realizatsiya-umnyih-setey-na-baze-komponentov-plc-ot-texas-instruments (In Russ.)

2. Devendran S., Misra A., Mishra S. [Power supply for wireless dimmer without neutral: Typical design and testing]. *Novosti elektroniki* = Electronics News. 2017; 2:33–43. Available at: https://www.terraelectronica.ru/files/news/NE_02_2017_s33.pdf (In Russ.)

3. Kondratyev V. [Communication on electrical networks: principles, standards, applications]. *Elektronnyye komponenty* = Electronic Components. 2011; 12:40–44. Available at: http://ns1.russianelectronics.ru/leader-r/review/2327/doc/57948 (In Russ.)

4. Zusev S. A. Using the wired and wireless interfaces to energy facilities, the example of PLS systems and ZigBee wireless interface. *Sovremennyye nauchnyye issledovaniya i innovatsii* = Modern Scientific Research and Innovations. 2016; 4. Available at: http://web.snauka.ru/issues/2016/04/67031 (In Russ.)

5. Kolokolnikova A. I., Karnaukhov D. V. Application of automated information data systems in domestic household. *Problemy sovremennoy nauki* = Problems of Modern Science. 2013; 8-1:109–116. Available at: https://elibrary.ru/item.asp?id=19144150 (In Russ.)

6. Borisov R. K., Kovalev D. I., Kokorin S. A., Kochurov O. M. [Application of Yitran PLC-technologies in the control system of safety locks of high voltage switchgears]. *Elektrichestvo* = Electricity. 2014; 12:18–23. Available at: https://elibrary.ru/item.asp?id=22490944 (In Russ.)

7. Balaev A. A., Gorbatov V. S., Sepashvili D. T. Safety testing of PLC-data transmission technology. *Bezopasnost informatsionnykh tekhnologiy* = Information Security. 2011; 1:57–60. Available at: https://elibrary.ru/item.asp?id=18813084 (In Russ.)

8. Balaev A. A., Gorbatov V. S. The problem of special research facilities PLC-networks in the validation tests for safety information is considered. *Bezopasnost informatsionnykh tekhnologiy* = Information Security. 2012; 1:79–80. Available at: https://elibrary.ru/item.asp?id=18811100 (In Russ.)

9. Shchagin A. V., Zo N. L., Lvin V. Ya., Khtut P. Kh. Methods of providing the reliability of information transmission in information-management PLC-networks of enterprises. *Informatsionnyye sistemy i tekhnologii* = Information Systems and Technologies. 2014; 83(3):107–113. Available at: http://elibrary.ru/item.asp?id=21574904 (In Russ.)

10. Shikov S. A. Problems of information security: Internet of Things. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2017; 1(27):27–40. DOI: 10.15507/0236-2910.027.201701.027-040 (In Russ.)

Submitted 19.10.2017; revised 20.12.2017; published online 20.03.2018

About the authors:

Sergey N. Ivliyev, Head of Information Security and Service Chair, Institute of Electronics and Lighting Engineering, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russia), Ph.D. (Engineering), ResearcherID: E-1697-2014, ORCID: http://orcid.org/0000-0002-6101-3388, ivliev_sn@mail.ru

Svetlana L. Krylova, Senior Lecturer, Information Security and Service Chair, Institute of Electronics and Lighting Engineering, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russia), ResearcherID: L-7324-2017, ORCID: http://orcid.org/0000-0003-4083-9209, svet711@yandex.ru

Stanislav A. Shikov, Lecturer, Information Security and Service Chair, Institute of Electronics and Lighting Engineering, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russia), ResearcherID: S-2514-2016, ORCID: http://orcid.org/0000-0002-8412-5163, stenlav@mail.ru

Contribution of the co-authors:

S. N. Ivliyev: scientific leadership, developing the concept of the threat model, analysing the initial data; S. L. Krylova: adaptation and actualization of the threat model, construction of an adapted threat model taking into account the requirements of regulators; S. A. Shikov: layout of the article, preparation of graphic material, analytical processing of normative documentation.

All authors have read and approved the final version of the manuscript.