УДК 621.391

# СХЕМЫ УПРАВЛЕНИЯ КЛЮЧАМИ С ИСПОЛЬЗОВАНИЕМ КАДРОВ МАРШРУТНОЙ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ SCADA-СИСТЕМ

***Камаев Валерий Анатольевич,*** доктор технических наук, профессор, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28, тел.: +7 (8442) 24-81-00, e-mail: kamaev@unix.cad.vstu.ru

***Куанг Винь Тхай,*** директор, Институт информационной технологии, Вьетнам, г. Ханой, e-mail: tqvinh@ioit.ac.vn

***Финогеев Алексей Германович,*** доктор технических наук, профессор, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40, тел. +7 (927) 289-93-63, e-mail: finogeev@sura.ru

***Нефедова Ирина Сергеевна,*** аспирант, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40, тел. +7 (987) 505-94-54, e-mail: nefedya2008@yandex.ru

***Финогеев Антон Алексеевич,*** кандидат технических наук, доцент, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40, тел. +7 (927) 090-23-50, e-mail: antonfinogeev@mail.ru

***Ботвинкин Павел Викторович,*** аспирант, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28, тел. +7 (905) 394-21-88, e-mail: pavel.botvinkin@gmail.com

Функционирование автоматизированных систем управления в различных отраслях промышленности, транспорта, коммунальных услуг, научной деятельности и пр. осуществляется на основе компьютерных технологий. От степени защищённости этих систем во многом зависит не только успешность работы организаций, но и безопасность регионов, национальная безопасность. Поэтому защита корпоративных информационных систем от угроз безопасности является важным элементом реализации практически любого IT-проекта, в том числе и систем диспетчерского контроля и сбора данных. От соответствия сведений, предоставляемых SCADA-системами, требованиям достоверности и оперативности зависит эффективность функционирования различных организаций, причем для некоторых их типов – в решающей степени. В статье рассмотрено содержание термина «SCADA-системы» и приведено обоснование необходимости обеспечения их безопасности. Исследуются проблемы, цели и задачи управления ключами при шифровании данных в беспроводных сенсорных сетях (WSN) SCADA-систем. Исследована структура ключевой информации в сети ZigBee и возможные методы получения ключей участниками взаимодействия. Обоснована целесообразность применения гибридной схемы шифрования и управления ключами в WSN, когда сеансовый симметричный ключ используется для шифрования данных, а асимметричные ключи – для шифрования сеансового ключа. Для решения проблемы аутентификации узлов, с которых поступает информация в сеть, и верификации данных в качестве электронной цифровой подписи используются хеш-функции. Предложены три методики гибридного управления ключами, зависящие от метода маршрутизации и топологии WSN с передачей ключевой информации вместе с маршрутными кадрами. Проанализированы достоинства и недостатки этих методик для различных условий использования.

**Ключевые слова:** обеспечение безопасности, беспроводная сенсорная сеть, SCADA-система, управление ключами, шифрование данных, WSN, маршрутизация, ассиметричное и симметричное шифрование, гибридная схема шифрования

**PRIKASPIYSKIY ZHURNAL: Upravlenie i Vysokie Tekhnologii**
**(CASPIAN JOURNAL: Management and High Technologies), 2014, 3 (27)**
**INFORMATION-MEASURING, REFERENCE, EXPERT-ANALYTICAL SYSTEMS**

# ROUTING AND MANAGING ENCRYPTION KEYS IN WIRELESS SENSOR NETWORKS OF SCADA SYSTEMS

***Kamaev Valeriy A.,*** D.Sc. (Engineering), Professor, Volgograd State Technical University, 28 Lenin av., Volgograd, 400005, Russian Federation, phone: +7 (8442) 24-81-00, e-mail: kamaev@unix.cad.vstu.ru

***Kuang Vin Thay,*** Director, Institute of Information Technology, Hanoi, Vietnam, e-mail: tqvinh@ioit.ac.vn

***Finogeev Alexey G.,*** D.Sc. (Engineering), Professor, Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation, phone: +7 (927) 289-93-63, e-mail: finogeev@sura.ru

***Nefedova Irina S.,*** postgraduate student, Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation, phone: +7 (987) 505-94-54, e-mail: nefedya2008@yandex.ru

***Finogeev Anton A.,*** Ph.D. (Engineering), Associate Professor, Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation, phone: +7 (927) 090-23-50, e-mail: antonfinogeev@mail.ru

***Botvinkin Pavel V.,*** postgraduate student, Volgograd State Technical University, 28 Lenin av., Volgograd, 400005, Russian Federation, phone: +7 (905) 394-21-88, e-mail: pavel.botvinkin@gmail.com

Functioning of the automated control systems in various branches of industry, transport, utilities, and other scientific activities is carried out on the basis of computer technology. One the degree of vulnerability of these systems depends not only the success of organizations, but also the security of regions, national security. Therefore, protection of corporate information systems from security threats is an important element of nearly any IT-project, including systems for supervisory control and data acquisition. On compliance of information, provided by the SCADA-systems, to the requirements of reliability and efficiency, depends the effective functioning of the whole enterprise. This article discusses the definition of term "SCADA-systems" and explains the need to ensure their safety. The paper examines the problems, goals and objectives of key management in the data encryption at wireless sensor networks (WSN) SCADA systems. The structure of the key information in the ZigBee network and methods receiving the keys. The application of the hybrid encryption and managing encryption keys in WSN, when a session symmetric key used to encrypt data, and asymmetric keys to encrypt the session key. To solve the problems of authentication and verification data hash function is used. Proposed three schemes of hybrid managing encryption keys, depending on the routing method and WSN topology with the transfer of key information in the route frames. Analyzed advantages and disadvantages of these methods for different conditions of use.

**Keywords:** security, wireless sensor network, SCADA systems, managing encryption keys, data encryption, routing, asymmetric and symmetric encryption, hybrid encryption scheme

**Введение.** Функционирование автоматизированных систем управления в различных отраслях промышленности [3], транспорта, коммунальных услуг, научной деятельности и пр. осуществляется на основе компьютерных технологий. От степени защищённости этих систем во многом зависит не только успешность и прибыльность работы организаций, но и безопасность регионов, национальная безопасность [10].

Широкое и всё возрастающее внедрение автоматизации практически во все сферы деятельности привело к коренной перестройке измерительной техники: теперь в её задачу наряду с измерениями входит также информационное обслуживание исследуемого (контролируемого) объекта. Оно включает автоматический сбор, представление, доставку, запоминание, регистрацию, отображение, обработку и анализ информации, полученной в результате отдельных измерений [11].

Целью данной работы является повышение уровня информационной безопасности систем диспетчерского управления и сбора данных путём анализа эффективности методов

управления ключами с использованием кадров маршрутной информации в беспроводных сенсорных сетях этих систем.

**SCADA-системы.** В узком смысле под термином «SCADA-система» (SCADA — Supervisory Control And Data Acquisition) иногда подразумевается только программное обеспечение автоматизированных систем управления технологическими процессами (АСУ ТП), в широком смысле — любая система, оперирующая передаваемыми по коммуникационным каналам сигналами и управляющая удалённым оборудованием [9, 21, 38].

Под указанное толкование термина «SCADA-система» подпадает большое число разнородных систем: промышленные системы управления производством, энергетические [19, 39] системы (государственные, региональные, муниципальные, локальные, системы управления атомными электростанциями [17] и т.д.), системы мониторинга и диспетчерского управления транспортом (наземным, подземным, воздушным, водным); различные военные и стратегические автоматизированные системы; системы управления космическими аппаратами; всевозможные программно-аппаратные автоматизированные комплексы [7, 20] и т.д.

Потенциально важным, но пока слабо развитым в России направлением применения SCADA-систем можно считать дистанционный мониторинг и управление (в перспективе – автоматизированное) в отношении мобильных пациентов медучреждений, прежде всего входящих в «группы риска». Такой мониторинг может осуществляться с помощью носимых пациентами сенсорных и приемо-передающих систем, в том числе и в автоматизированном режиме. При этом вопросы ИБ важны в отношении таких видов информации: персональный состав (список) мониторируемых пациентов; содержание собираемой/передаваемой медицинской информации; сведения о перемещении мониторируемых пациентов в «пространстве-времени»; управляющие воздействия или указания, направленные на корректировку возникших патологических состояний или их предотвращение [6, 13].

Эффективность решения задач по обеспечению информационной безопасности (ИБ) АСУ ТП и SCADA-систем в значительной степени зависит от применяемых технологий и средств защиты компонентов транспортной среды передачи данных [26, 27].

SCADA-системы используют проводные и/или беспроводные сенсорные сети (Wireless Sensor Network – WSN) в качестве транспортной среды сбора телеметрической информации и пересылки команд на исполнительные устройства [25].

Традиционные меры обеспечения ИБ (использование сложных алгоритмов шифрования, многофакторной аутентификации, антивирусных программ, межсетевых экранов и т.п.) не всегда применимы в силу ограниченных вычислительных и энергетических ресурсов сенсорных узлов и беспроводной сенсорной сети (WSN) в целом. Кроме того, производители приборов промышленной автоматики и исполнительных устройств разрабатывают закрытые протоколы их функционирования, которые не позволяют внедрить технологии защиты с использованием IPSec, SSL, VPN и т.п. [34].

На большинстве предприятий, использующих системы диспетчерского управления и сбора данных отсутствуют процедуры управления инцидентами безопасности и их анализа, а также не разработаны мероприятия, препятствующие повторному возникновению опасных событий [29].

**Общая характеристика проблематики защиты корпоративных информационных систем от угроз информационной безопасности.** Первой серьёзной направленной угрозой на область SCADA-систем стал вирус Stuxnet, атаковавший ядерные объекты Ирана. Влияние появления (обнаружения) этого вируса было признано настолько весомым, что сейчас принято разделять историю безопасности промышленных систем на два этапа: до появления Stuxnet и после [1]. В ходе анализа вируса стало известно, что он

проектировался специально под SCADA-систему фирмы Siemens – SIMATIC WinCC, которая эксплуатировалась на АЭС в Бушере. Эта же система (WinCC) используется, например, в скоростных поездах, на российских химзаводах, на компрессорных станциях Газпрома и др. Поэтому угрозы, связанные с вирусами Stuxnet важны с позиций региональной и национальной безопасности России, а не только зарубежных стран и корпораций, которые выпускают или используют соответствующее оборудование.

Спецслужбы иностранных государств [22], конкурирующие корпорации или кибертеррористы могут использовать в своих целях недостаточное внимание к обеспечению информационной безопасности АСУ ТП [8] и их компонентов [18] со стороны руководства организаций, их «профильных» сотрудников.

Важным «стимулирующим» фактором для российских специалистов в области ИБ является также появление новых требований регулирующих органов и организаций, направленных на повышение безопасности промышленных систем [4, 10].

Защита корпоративных информационных систем от угроз безопасности является важным элементом реализации практически любого IT проекта, в том числе и систем диспетчерского контроля и сбора данных [28]. От соответствия сведений, предоставляемых SCADA-системами, требованиям достоверности и оперативности зависит эффективное функционирование предприятий [5, 12].

SCADA-системы используют проводные или беспроводные сенсорные сети (WSN) в качестве транспортной среды сбора телеметрической информации и пересылки команд на исполнительные устройства [27]. Большинство таких систем не подключены напрямую к интернету с низким уровнем безопасности [31, 32, 33]. Однако обычно они соединены с бизнес-системам предприятия (MRP, управление запасами и т.д.), с коммуникациям технического обслуживания производителями и консультантами, которые подключены к внешним сетям. Даже если использовать технологию физической изоляции («воздушного зазора» – air gap) критической SCADA-системы, то она все равно будет находиться в зоне риска, потому что современные системы управления нуждаются в поступлении регулярной электронной информации из внешнего мира. Введение мер физической изоляции порождает новые пути нарушения информационной безопасности, которыми труднее управлять. Например, вирус Stuxnet проходил сквозь брандмауэры АСУ ТП либо по косвенным путям (таким как USB-ключи и компакт-диски), либо посредством протоколов, пропускаемых межсетевыми экранами в силу их настроек.

Поэтому целью обеспечения безопасности SCADA-системы должно быть не создание «воздушного зазора», а реализации архитектуры, которая защищает систему управления от внешних атак и повышает стойкость каждой сенсорной сети, канала связи, отдельных устройств и кадров данных [15].

Современная тенденция к организации транспортной среды SCADA-систем определяет использование беспроводных самоорганизующихся сетей, особенностями которых являются равноправность узлов, динамически изменяющаяся топология, возможность реконфигурации сети, самовосстановление, динамическая маршрутизация и т.д. В частности, технология ZigBee предоставляет хорошую основу для построения надежных беспроводных сетей сбора данных [25]. Такие сети постепенно вытесняют нетехнологичные проводные сети и находят применения в промышленности для управления технологическим оборудованием [28], в коммунальном хозяйстве для управления теплоснабжением [23, 24], освещением, кондиционированием и вентиляцией [39, 40], коммерческого учета потребленной энергии и воды, в системах пожарной безопасности, в системах домашней автоматизации, в медицинских системах мониторинга и т.п.

В плане обеспечения надежной и безопасной передачи данных беспроводная транспортная среда SCADA-системы [30] должна быть устойчивой как к радиопомехам, так

и к различным видам воздействий, которые потенциально могут привести к нарушению ее функциональности, сбоям и отказам в работе сетевых узлов и подключенным к ним устройств. Обеспечение помехоустойчивости требует реализацию мероприятий по электромагнитной защите узлов сети (их экранирование, использование узконаправленных антенн для передачи информации, применение фильтров помех, помехоустойчивое кодирование данных, расширение спектра частот по методу прямой последовательности, активная смена радиоканалов, динамическая маршрутизация), что позволяет устранить или существенно снизить влияние помех, независимо от того, вредоносные они или нет.

Для защиты от других видов воздействий требуются программно-аппаратные методы реализации модели многослойной защиты компонент SCADA-системы и обеспечение безопасности сетевого взаимодействия в условиях общедоступной беспроводной передачи данных. Так как сенсорные узлы WSN имеют ограниченные вычислительные и энергетические ресурсы, то невозможно в полной мере использовать традиционные способы защиты информации, принятые в компьютерных сетях. Задача обеспечения безопасности сенсорных сетей смещается в область создания защищенных каналов передачи данных, использования современных технологий аутентификации, верификации, шифрования и управления ключами, предотвращения утечек данных из системы, обнаружения вторжений и атак [16], использования алгоритмов динамической маршрутизации [1] и т.п.

**Управление ключами при шифровании данных в WSN SCADA-систем.** Современные криптографические системы защиты данных работают на основе использования технологий шифрования с применением симметричных ключей или асимметричных закрытых и открытых ключей. Для аутентификации элементов SCADA-системы и узлов сенсорной сети применяются специальные секретные коды для контроля целостности передаваемых данных на основе использования хеш-функции. Кроме того, в SCADA-системах используется множество паролей доступа к различным устройствам, которые требуется периодически изменять с целью снижения вероятности их компрометации. Таким образом, в сложной системе имеется много секретной информации, с которой требуется постоянно работать с целью исключения либо снижения вероятности ее компрометации, что приводит к необходимости разработки и внедрения системы управления ключами.

Если алгоритмы криптографического преобразования данных достаточно хорошо проработаны с точки зрения надежности защиты информации, то процедуры безопасного создания, использования и обмена ключами являются проблемными задачами. Неправильное использование ключей приводит к компрометации системы информационной безопасности, так как криптостойкость системы шифрования в большей степени зависит от конфиденциальности ключей.

Существуют две проблемы, связанные с процедурами управления ключами.

1. Как сгенерировать ключи, обладающими необходимыми криптографическими свойствами?
2. Как безопасно передать их по беспроводной транспортной среде сенсорной сети участникам информационного взаимодействия?

В беспроводных сенсорных сетях решение этих задач усложняется из-за отсутствия фиксированных маршрутов передачи данных – в силу самоорганизации сети, спонтанности соединений при построении маршрутов, случайного характера информационных взаимодействий между сенсорными узлами.

В общем случае целью управления ключами является нейтрализация угроз компрометации конфиденциальности закрытых ключей, аутентичности закрытых или

открытых ключей, несанкционированного использования закрытых или открытых ключей, исключения использования ключей с истекшим сроком действия. Основной задачей системы управления ключами является обеспечение участников информационного взаимодействия в беспроводной сенсорной сети (WSN) SCADA-системы ключевыми данными для реализации конфиденциального обмена информацией по защищенным каналам связи.

Основные процедуры управления ключами, которые должны быть реализованы в системе, следующие.

1. Регистрация узлов сети как участников взаимодействия.
2. Генерация ключей с необходимыми криптографическими качествами.
3. Накопление, хранение и учет ключей.
4. Ввод ключей в телекоммуникационную среду SCADA-системы.
5. Распределение ключей между узлами сенсорной сети.
6. Управление связями между участниками информационного обмена и ключами.
7. Замена ключей.
8. Вычисление хеш-функций для аутентификации участников.
9. Восстановление ключей в случае их случайного уничтожения.
10. Уничтожение ключей по плану или в случае их компрометации.

**Структура ключевой информации в WSN технологии ZigBee.** Механизмом конфиденциальности в сенсорных сетях ZigBee является шифрование и защита ключевых данных при установлении доверительных отношений между взаимодействующими сторонами – как на стадии установки ключей, так и в процессе передачи данных [42]. Структура безопасности регламентируется стандартом IEEE 802.15.4, где безопасность приложений обеспечивается посредством их профилей. Прежде всего, спецификация ZigBee Pro Feature Set поддерживает шифрование данных, определяет способы изменения, рассылки и шифрования ключей [35]. Кроме того, может использоваться протокол дополнительного шифрования на уровне приложений при обмене данными между двумя узлами в сети, которые не могут быть расшифрованы ни одним другим узлом сети – несмотря на то, что все они имеют общий сетевой ключ.

Система безопасности в соответствии со спецификацией ZigBee основана на AES алгоритме симметричного шифрования со 128-битными ключами, которые могут ассоциироваться с сетью (ключ сети) или с каналом связи (ключ соединения). Создание ключей основано на использовании главного ключа (Master Key – MK), который контролирует их соответствие. Первоначальный главный ключ должен быть получен через безопасную среду (передачей или предварительной установкой).

В защищенной сети ZigBee назначается центр управления ключами, которому другие узлы доверяют распределение ключей. В идеале каждый узел сети должен иметь предварительно загруженный адрес данного центра, чтобы получать от него ключ сети (Network Key – NK) и сеансовые ключи соединения (Link Key – LK). На этапе конфигурации или реконфигурации сети центр управления безопасностью разрешает или запрещает присоединение к сети новых устройств, т.е. работает со списками контроля доступа ACL. Обычно центром управления по совместительству является координатор сети, но это может быть, связанный с ним сервер. Таким образом, в WSN данного стандарта используются три типа ключей.

1. Главный ключ MK применяется не для шифрования, а как первоначально разделяемый двумя узлами секретный код при выполнении процедуры генерации сеансового ключа соединения.

2. Ключ сети NK обеспечивает безопасность на сетевом уровне, он имеется у каждого устройства в сети. Данные ключи используются при отключении и последующем

повторном подключении узлов к сети. В процессе работы центр управления ключами может периодически обновлять ключ сети, и транслировать всем узлам новый ключ, зашифрованный с помощью старого ключа. Сетевые ключи высокой безопасности передаются в зашифрованном виде, а обычные ключи – незашифрованными.

3. Сеансовые ключи соединения LK обеспечивают безопасную одноадресную передачу кадров между узлами на уровне приложений.

Так как безопасность сетей ZigBee основана на симметричных ключах, то отправитель и получатель кадра данных должны иметь один общий ключ, который используется при шифровании/дешифровании. Есть три метода получения ключей участниками информационного обмена: предварительная установка; передача от центра управления ключами; синтез ключей участниками взаимодействия. В случае предварительной установки ключи помещаются в узлы или PLC (Programmable Logic Controller – программируемый логический контроллер) заранее путем занесения их в прошивку устройства, передачи по кабелю при конфигурировании и т.п. Во втором случае центр управления ключами пересылает ключи устройствам (настолько безопасным методом, насколько это возможно). В третьем случае один из участников взаимодействия самостоятельно генерирует ключи перед информационным обменом и отсылает партнеру.

При использовании технологии симметричного шифрования участникам информационного обмена передается одинаковый ключ (Shared key – SK) для шифрования и расшифровки, что вызывает две проблемы.

1) Необходимость надёжной передачи ключей каждому абоненту по секретному или защищенному каналу.

2) Сложность управления ключами, что означает квадратичное возрастание числа ключей, которые надо генерировать, передавать, хранить и уничтожать для каждой пары узлов в сенсорной сети.

Для решения данных проблем в сетевых системах используется схема ассиметричного шифрования с открытым ключом. Открытый ключ передаётся по незащищённому каналу связи отправителю и используется для шифрования сообщений, а закрытый остается у получателя и используется для расшифровки. Для связи двух ключей используются односторонние функции, то есть такие функции $y = f(x)$, для которых по известному значению $x$ достаточно просто найти значение $y$. В то же время определить $x$ по известному значению $y$ за разумное время практически невозможно – даже при использовании современных аппаратно-программных средств.

Использование асимметричных алгоритмов снимает проблему распределения ключей в системе, но ставит задачу подтверждения достоверности полученных ключей и аутентификации их источника – особенно в беспроводных сетях, где возможна подмена центра генерации ключей с последующим получением всей зашифрованной информации. Для решения проблемы аутентификации используется технология электронной цифровой подписи, когда сообщение предварительно подвергается хешированию с помощью закрытого ключа, а другая сторона с помощью открытого ключа может проверить подлинность подписи получателя. Подобная схема совместного применения ассиметричного шифрования и цифровой подписи используется в криптосистеме RSA [37], где отправитель сначала добавляет к сообщению свою цифровую подпись, а затем – шифрует сообщение и подпись с помощью открытого ключа принадлежащего получателю. Получатель расшифровывает полученное сообщение с помощью закрытого ключа, проверяя как подлинность отправителя, так и целостность сообщения.

Несмотря на то, что данные методы решают проблемы симметричных схем, связанные с начальной передачей ключа другой стороне и с синхронизацией ключей, такие системы требовательны к длине ключей, вычислительным ресурсам сетевых узлов, производительности всей сети – эти причины не позволяют применять их в сенсорных сетях.

Поэтому для использования в сенсорной сети SCADA-систем больший интерес представляет гибридная (комбинированная) система шифрования, совмещающая преимущества ассиметричной криптосистемы с производительностью симметричных криптосистем. Здесь сеансовый симметричный ключ используется для шифрования данных, а асимметричный алгоритм используется для шифрования сеансового ключа. Таким образом, структуру ключей, принятую в стандарте ZigBee, следует дополнить еще одним типом ключей (Asymmetric Key – AK), которые будут использоваться для шифрования симметричных сеансовых ключей соединения (рис. 1).

Главный ключ, сетевые ключи и, возможно, ключи для шифрования сеансовых ключей являются ключами с длительным сроком действия. В то же время сеансовые ключи шифрования данных, как правило, имеют короткий период использования.

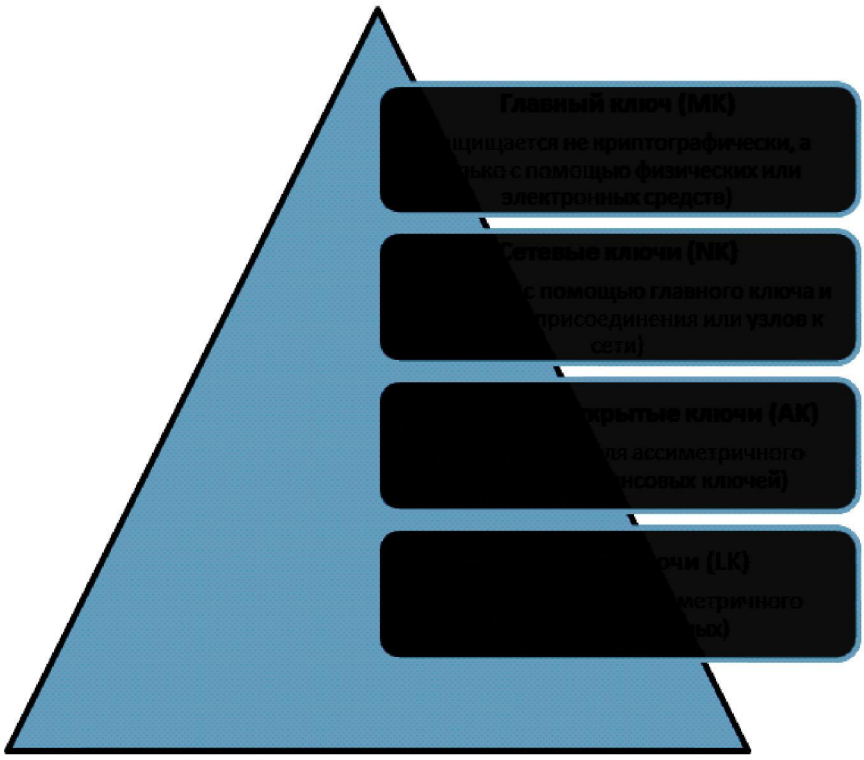


Рис. 1. Структура ключей для гибридной схемы защиты данных в WSN

Принципы работы такой системы будут различаться в зависимости от используемого алгоритма маршрутизации, так как предлагается процедуру обмена ключами проводить вместе с передачей маршрутной информации и квитанций подтверждения – с целью сокращения объема служебного трафика.

**Основные типы протоколов управления ключами в WSN.** В современных SCADA-системах наиболее распространенной (в силу простоты реализации) является транспортная среда WSN с централизованным механизмом управления. При этом сеть имеет топологическую структуру «звезда» или «кластерное дерево» и существует только один

координатор, который непосредственно связан через шлюз с сервером АСУ технологическим процессом (ТП). Поэтому логично устанавливать систему управления ключами именно на данном сервере.

Более сложной является задача управления ключами в сетях децентрализованного или частично децентрализованного типа, где есть несколько координаторов, отвечающих за работу доверенных зон (адресных пространств) сенсорной сети, которые взаимодействуют друг с другом. В случае большой распределенной сети с топологией ячеистого типа (mesh) можно использовать несколько подсистем управления ключами для каждой зоны, но с синхронизируемыми базами ключей, располагающихся на доверенных серверах. Однако, сложность задачи управления ключами линейно возрастает с ростом количества доверенных зон и сенсорных узлов в них. Кроме обеспечения безопасного и защищенного информационного взаимодействия сенсорных узлов, промышленных контроллеров и координаторов зоны, добавляются задачи обеспечения безопасного взаимодействия координаторов друг с другом и задача обеспечения репликации баз ключей, расположенных на серверах.

В общем случае, протоколы управления ключами можно разделить на три большие группы: протоколы предварительного размещение ключей; арбитражные протоколы с третьей доверенной стороной; автономные (самодостаточные, самоутверждающие) протоколы.

Протоколы с предварительным размещением ключей позволяют снизить служебный трафик в сенсорной сети, так как ключи заранее помещаются в прошивку при конфигурировании сенсорных узлов вместо открытой передачи их по сети. Недостатком является потеря гибкости и невозможность оперативной замены ключей в случае их компрометации.

В арбитражных протоколах для генерации, распределения, установки и поддержания ключей используется третья доверенная сторона, установленная на координаторе или связанном с ним сервере, которая решает основные задачи управления ключами. В процессе информационного обмена третья доверенная сторона играет следующие роли (рис. 2).

Система безопасности, установленная на данном устройстве, генерирует, хранит и распределяет ключи; производит учет, адресацию и конфигурацию сетевых сенсорных узлов; отвечает за их авторизацию. В случае компрометации системы управления ключами полностью теряется контроль над работой SCADA-системы.

Автономные протоколы работают по схеме самостоятельного распределения парных одинаковых ключей между взаимодействующими сторонами (симметричное шифрование), либо передачи открытого ключа одной из сторон с хранением закрытого ключа у другой стороны (ассиметричное шифрование) перед началом информационного обмена.


Рис. 2. Роли третьей доверенной стороны

Основными недостатками в первом случае является передача ключа для расшифровки другой стороне по беспроводным небезопасным каналам связи с возможностью его перехвата и компрометации; квадратичный рост количества ключей в зависимости от числа участников взаимодействия. Во втором случае недостатками являются вычислительная сложность алгоритмов генерации парных ключей; большая размерность ключей; сложность шифрования/расшифровки и необходимость аутентификации узла генерации ключей. Эти факторы приводят к значительным затратам времени и энергии для сенсорных узлов с ограниченными вычислительными и энергетическими ресурсами.

Поэтому наиболее эффективной является система гибридного шифрования, где пары ассиметричных ключей используются для шифрования симметричного ключа перед его передачей участникам взаимодействия с аутентификацией инициатора передачи посредством хеш-функции в виде электронной цифровой подписи. Однако ее применение не исключает роста объема служебного трафика, вызванного необходимостью обмена ключевой информацией.

В SCADA-системах используются все типы протоколов, в частности, производители устанавливают пароли для доступа/конфигурирования устройств и сетевых узлов; секретные коды для аутентификации узлов и передаваемых кадров данных; схемы вычисления хеш-функций.

**Схемы гибридного управления ключами при шифровании данных в WSN технологии ZigBee.** В традиционных беспроводных сетях проблема защиты передаваемых данных обеспечивается сервисами и службами на программном уровне. С точки зрения безопасности сенсорные сети не отличаются от других типов беспроводных сетей. Они уязвимы для атак пассивного прослушивания и атак активной фальсификации, так как беспроводная среда общедоступна. Более того, ограниченные энергоемкость, вычислительная мощность и оперативная память узлов не позволяют обеспечить достаточно надежную защиту передаваемых данных. Такие ограничения сужают выбор и использование криптографических механизмов и протоколов на канальном и физическом уровнях сетевой

модели. Как следствие, это требует реализации архитектурных компонент системы безопасности на сетевом и прикладном уровнях.

***Автономная схема гибридного управления ключами при динамической маршрутизации AODV в WSN ячеистой топологии.*** Первым методом является использование реактивного протокол динамической маршрутизации «Ad hoc On Demand Distance Vector» (AODV) дистанционно-векторного типа. Он в основном применяется в сенсорных сетях ячеистой топологии (mesh) и устанавливает маршрут от источника до адресата по широковещательным запросам [2]. Когда один из сенсорных узлов собирается передать данные, он посылает широковещательный запрос на создание маршрута (Route Requests – RREQ). Маршрутизаторы сенсорной сети широковещательно ретранслируют кадр и делают в своих таблицах маршрутизации запись об узле, от которого они приняли запрос. В кадр также записывается «логическое расстояние» от отправителя запроса до текущего положения. В сенсорной сети с ячеистой топологией узел-адресат получит несколько кадров RREQ с различными «логическими расстояниями». Узел-адресат отправляет ответ (Route Reply – RREP) тому устройству, от которого пришел пакет с минимальным «логическим расстоянием» и далее по кратчайшей цепочке RREP передается маршрутизаторами, пока не достигнет источника. Таким образом, ответ, возвращаясь по оптимальному пути, формирует таблицу прямого маршрута для передачи кадров от источника до адресата. Если связь ненадёжная, то предусмотрена возможность передачи квитанции подтверждения маршрута от узла-инициатора адресату (RREP-ACK).

С целью снижения служебного трафика объединим процедуры управления ключами по автономному протоколу, добавляя соответствующие поля для открытого ключа и хэш-функции в маршрутные кадры RREQ и RREP. Тогда методика автономного гибридного управления ключами при шифровании кадров данных и аутентификации отправителя будет следующей.

1. Отправитель генерирует случайный сеансовый ключ для алгоритма AES длиной 128 бит, с помощью которого шифруется и готовится к отправке кадр данных.

2. Отправитель отсылает широковещательный запрос на создание маршрута RREQ и на получение открытого ключа от адресата для шифрования сеансового ключа.

3. Получатель генерирует случайную пару «открытый ключ – закрытый ключ» по алгоритму RSA и отсылает открытый ключ отправителю вместе с маршрутным ответом RREP. Для аутентификации получателя вычисляется хеш-функция кадра с открытым ключом; затем шифруется ключом, известным обеим сторонам и также передается вместе с кадром.

4. Отправитель шифрует сеансовый ключ открытым ключом и посылает его получателю вместе с зашифрованным сеансовым ключом кадром данных. Для аутентификации отправителя и верификации данных в кадре вычисляется хеш-функция зашифрованного кадра, которая шифруется ключом, известным обеим сторонам и передается вместе либо вместе с кадром данных, либо вместе с квитанцией подтверждения маршрута RREP-ACK при плохом качестве канала связи.

5. Получатель расшифровывает сеансовый ключ и хеш-функцию, проверяет подлинность отправителя и целостность зашифрованного кадра. Далее расшифровывает кадр данных при помощи сеансового ключа и уничтожает этот ключ.

***Арбитражная схема гибридного управления ключами при иерархической маршрутизации в WSN кластерной топологии.*** Вторым методом маршрутизации в сетях ZigBee кластерной топологии является иерархическая маршрутизация, которая сводится к передаче от источника к получателю вдоль ветвей кластерного дерева с учетом родительских и дочерних взаимосвязей [41]. При построении кластерных деревьев ZigBee

сети [35] координатор, а затем присоединенные к нему маршрутизаторы, присваивают диапазоны адресов дочерним устройствам в иерархическом порядке. В результате каждый узел может определить, принадлежит ли адрес получателя кадра данных к его «дочерним» ветвям или находится в другой части сети и, следовательно, передача должна проводиться через общий корневой узел дерева или координатор всей сети.

При такой топологии сенсорной сети и способе иерархической маршрутизации целесообразно использование протокола управления ключами арбитражного типа, где на сетевом координаторе или связанном с ним сервере SCADA-системы реализована роль доверенного сертифицирующего центра в схеме гибридного шифрования. Методика арбитражного гибридного управления ключами при шифровании кадров данных и аутентификации отправителя будет следующей.

1. Присоединяемые к сенсорной сети узлы получают от координатора или маршрутизаторов адреса в соответствии с диапазонами для ветвей кластерного дерева.
2. Каждый вновь присоединяемый узел генерирует случайную пару «открытый ключ – закрытый ключ» по алгоритму RSA и отсылает кадры с открытым ключом, адресом и вычисленной хеш-функцией в качестве цифровой подписи центру управления ключами. Последний записывает во внутреннюю память и хранит записи с открытыми ключами, адресами и цифровыми подписями сенсорных узлов. Закрытые ключи хранятся в сенсорных узлах.
3. Перед передачей данных узел-источник отсылает запрос центру управления ключами на генерацию и получение сеансового ключа для симметричного шифрования данных и адрес получателя кадра для передачи ему того же ключа.
4. Центр управления проверяет подлинность источника, генерирует сеансовый ключ соединения для алгоритма симметричного шифрования AES длиной 128 бит, находит в базе ключей открытые ключи источника и получателя, шифрует сеансовый ключ с добавлением цифровой подписи координатора посредством вычисления некоторой хеш-функции.
5. Зашифрованный открытыми ключами источника и получателя сеансовый ключ отсылается источнику и получателю, где также проверяется подлинность центра управления ключами и расшифровывается сеансовый ключ с помощью хранимых закрытых ключей.
6. Источник зашифровывает кадр с помощью сеансового ключа, уничтожает ключ и отправляет кадр получателю, который расшифровывает его с помощью того же ключа и затем также уничтожает его.

***Арбитражная схема гибридного управления ключами при маршрутизации Many-to-One в WSN.*** Третий вид маршрутизации в сети ZigBee учитывает специфику информационных потоков, которые передаются от множества оконечных узлов к одному или нескольким координаторам. Этот вид маршрутизации называется Many-to-One Routing. При использовании такого механизма центральный координатор периодически рассылает всем узлам широковещательный запрос (SINK_ADVERTISE). Каждый узел сети хранит в памяти только адреса ближайших узлов, которым нужно передать кадр данных, чтобы он достиг координатора или оконечного узла. Когда узел получает запрос типа SINK_ADVERTISE, он отсылает обратно кадр Route Record и ждет квитанцию подтверждения маршрута. Каждый маршрутизатор, ретранслируя данный кадр, добавляет в него информацию о маршруте. Таким образом, координатор получает полную информацию о маршруте (трассу) до узла-источника и использует ее для отправки квитанции подтверждения маршрута и при получении последующего кадра данных. Вместе с квитанцией координатор может послать узлу какую-либо дополнительную информацию, например, зашифрованный сеансовый ключ для симметричного шифрования.

Методика арбитражного гибридного управления ключами при шифровании кадров данных и аутентификации отправителя будет следующей.

1. Центральный координатор отправляет широковещательный запрос (SINK_ADVERTISE) и ждет в ответ кадры Route Record.

2. Сенсорный узел, получив запрос типа SINK_ADVERTISE, генерирует случайную пару «открытый ключ – закрытый ключ» по алгоритму RSA; формирует кадр Route Record, в который добавляет вместе с адресной информацией открытый ключ; вычисляет и добавляет хеш-функцию кадра для аутентификации и отсылает кадр координатору.

3. Координатор получает кадр с маршрутной информацией, адресом источника, его хеш-функцией и открытым ключом. Далее он генерирует сеансовый ключ соединения для алгоритма симметричного шифрования AES длиной 128 бит; шифрует его полученным открытым ключом; добавляет к квитанции подтверждения маршрута; вычисляет с помощью открытого ключа хеш-функцию для своей аутентификации; отправляет полученный кадр обратно источнику.

4. Сенсорный узел расшифровывает полученный сеансовый ключ с помощью закрытого ключа, проверяет подлинность отправителя путем вычисления и сравнения хеш-функции с отправленной.

5. Далее производится шифрование кадра данных сеансовым ключом и отправка кадра координатору. Сеансовый ключ после использования уничтожается.

6. Координатор расшифровывает полученный кадр тем же ключом и уничтожает его.

**Заключение.** Достоинством предлагаемых подходов является использование существующих процедур маршрутизации для одновременного обмена ключевой информацией – это позволяет не увеличивать энергопотребление непосредственно при передаче информации. Однако энергопотребление сетевых узлов все же возрастает, так требуются энергозатраты на выполнение процедур генерации, хранения и уничтожения ключей, вычисление хеш-функций, проверку подлинности отправителя и т.д. Также возрастает и размер передаваемых кадров с маршрутной информацией, но количество циклов приема передачи останется неизменным.

Главным недостатком способов управления ключами при гибридном и ассиметричном шифровании является возможность успешной атаки для подмены открытого ключа или узлов, где генерируются парные ключи для ассиметричного шифрования — это будет приводить к компрометации работы всей сенсорной сети. Процесс получения асимметричного открытого ключа получателя сообщения уязвим к атаке, в ходе которой атакующий вмешивается во взаимодействие между отправителем и получателем; может модифицировать трафик, передаваемый между ними. Поэтому открытый асимметричный ключ должен иметь цифровую подпись, для подтверждения подлинности его отправителя. Сегодня не существует такой системы, в которой можно было бы гарантировать подлинность открытого ключа и, тот факт, что отправитель ключа не скомпрометирован до момента его отправки.

На следующем этапе шифруется сеансовый ключ с использованием асимметричного алгоритма шифрования/дешифрования и асимметричного открытого ключа получателя. Зашифрованный сеансовый ключ присоединяется к кадру маршрутизации, который включает также добавленную электронную подпись. Весь пакет данных передается получателю по беспроводной незащищенной сенсорной сети, и, естественно, он также может являться объектом сниффер-атак.

Для решения данных проблем можно отказаться от криптографического шифрования сеансовых ключей алгоритмами большой вычислительной сложности, а вместо этого осуществить скрытную передачу открытой или даже зашифрованной ключевой информации

стеганографическими методами. Несмотря на то, что криптографические механизмы защиты, такие как широковещательная аутентификация и управление ключами, сегодня являются необходимым условием для обеспечения безопасности и устойчивости работы приложений сенсорных сетей, другие методы также требуют интенсивного изучения. Примерами таких методов является стеганографическое скрытие самого факта передачи секретной информации; использование технологий временных меток и синхронизации при генерации и раскрытии ключевой информации; определение и предотвращение утечек данных; обнаружение и предотвращение вторжений в сенсорную сеть и т.д.

**Список литературы**

1. Бершадский А. М. Классификация методов маршрутизации в беспроводных сенсорных сетях / А. М. Бершадский, Л. С. Курилов, А. Г. Финогеев // Изв. ВолгГТУ. Серия. Актуальные проблемы управления, вычислительной техники и информатики в технических системах. – 2012. – Т. 10, № 14. – С. 181–185.

2. Бершадский А. М. Обзор методов маршрутизации в беспроводных сенсорных сетях / А. М. Бершадский, Л. С. Курилов, А. Г. Финогеев // Изв. ВУЗов. Поволжский регион. Технические науки. – 2012. – № 1. – С. 47–58.

3. Брайс Э. IT-безопасность в промышленности. Глубокий анализ пакетов данных для SCADA-систем / Э. Брайс. – Режим доступа: http://issuu.com/cta-mag/docs/20134012 (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

4. Брумштейн Ю. М. Информационная безопасность региона: анализ содержания термина, моделей оценки и некоторых вопросов управления / Ю. М. Брумштейн, А. Н. Подгорный // Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика. – 2011. – № 1. – С. 24–29.

5. Брумштейн Ю. М. Комплексный анализ факторов информационной и интеллектуальной безопасности регионов / Ю. М. Брумштейн, А. Н. Подгорный // Информационная безопасность регионов. – 2011. – № 1 (8). – С. 8–14.

6. Брумштейн Ю. М. Анализ моделей и методов выбора оптимальных совокупностей решений для задач планирования в условиях ресурсных ограничений и рисков / Ю. М. Брумштейн, Д. А. Тарков, И. А. Дюдиков // Прикаспийский журнал: управление и высокие технологии. – 2013. – № 3 (23). – С. 169–180.

7. Варлатая С. К. Математические модели динамики возникновения и реализации угроз информационной безопасности / С. К. Варлатая, М. В. Шаханова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1–2. – С. 7–11.

8. Воронцов А. А. Автоматизированные системы управления технологическими процессами. Вопросы безопасности / А. А воронцов // JetInfo. – 2011. – № 5.

9. Гаврилов А. В. SCADA-системы : Сайт лаборатории «Гибридные Интеллектуальные Системы» / А.В. Гаврилов // НГТУ, кафедра АППМ. – Режим доступа: http://www.insycom.ru /html/metodmat/Automat2011/Lect6.pdf (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

10. Грицай Г. Безопасность промышленных систем в цифрах : Сайт компании Positive Technologies / Г. Грицай, А. Тиморин, Ю. Гольцев, Р. Ильин, С. Гордейчик, А. Карпин // Positive Technologies. – Москва, 2012. – Режим доступа: http://www.ptsecurity.ru/download /SCADA_analytics_russian.pdf (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

11. Гусинский А. В. Информационно-измерительные системы : учеб. пос. : в 2 ч. / А. В. Гусинский, А. М. Кострикин, В. А. Ворошень и др. – Минск : БГУИР, 2003. – Ч. 1 – 40 с.

12. Жабин С. А. Вопросы информационной безопасности автоматизированных систем коммерческого учета электроэнергии / С. А. Жабин // Алгоритмы, методы и системы обработки данных. – 2007. – № 12. – С. 75–80.

13. Захаров Д. А. Комплексное применение информационно-коммуникационных технологий в сфере телемедицины / Д. А. Захаров, Ю. М. Брумштейн. – Астрахань : Астраханский государственный университет, Изд. дом «Астраханский университет», 2013. – 133 с.

14. Камаев В. А. Разработка и применение модели автоматизированной системы управления информационными процессами к задаче мониторинга состояния оборудования / В. А. Камаев, В. В. Лежебоков // Вестник компьютерных и информационных технологий. – 2009. – № 9. – С. 18–22.

15. Камаев В. А. Анализ методов оценки качества функционирования и эффективности систем защиты информации на предприятиях электроэнергетики / В. А. Камаев, В. В. Натров // Изв. ВолгГТУ. Серия. Актуальные проблемы управления, вычислительной техники и информатики в технических системах. – 2007. – Вып. 1, № 1. – С. 67–69.

16. Камаев В. А. Методология обнаружения вторжений / В. А. Камаев, В. В. Натров // Изв. ВолгГТУ. Серия. Концептуальное проектирование в образовании, технике и технологии. – 2006. – Вып. 2, № 2. – С. 127–132.

17. Кондаков В. В. Информационная безопасность систем физической защиты, учета и контроля ядерных материалов : учеб. пос. / В. В. Кондаков, А. А. Краснобородько. – Москва : МИФИ, 2008. – 48 с.

18. Методы повышения надежности систем SCADA. – Режим доступа: http://automation-system.ru/news/item/scada-2-2-2-2-2-2-2-2-2-2-2-2.html (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

19. Митрейкин А. Некоторые аспекты обеспечения безопасности АСУ ТП в ТЭК России / А. Митрейкин // Информационные ресурсы России. – 2011. – № 4 .

20. Пахомов П. И. Технология поддержки принятия решений по управлению инженерными коммуникациями / П. И. Пахомов, В. А. Немтинов. – Москва : Машиностроение, 2009. – 124 с.

21. Системы диспетчерского управления сбора данных (SCADA-системы). – Режим доступа: http://www.mka.ru/?p=41524 (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

22. Техника для спецслужб. Бюро Научно-Технической Информации // Безопасность локальных сетей. – Режим доступа: http://www.bnti.ru/showart.asp?aid=792&lvl=04 (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

23. Финогеев А. Г. Система удаленного мониторинга и управления сетями теплоснабжения на основе беспроводных сенсорных сетей / А. Г. Финогеев, В. Б. Дильман, В. А. Маслов, А. А. Финогеев // Прикладная информатика. – 2011. – № 3 (33). – С. 83–93.

24. Финогеев А. Г. Оперативный дистанционный мониторинг в системе городского теплоснабжения на основе беспроводных сенсорных сетей / А. Г. Финогеев, В. Б. Дильман, А. А. Финогеев, В. А. Маслов // Изв. ВУЗов. Поволжский регион. Технические науки. – 2010. – № 3. – С. 27–36.

25. Финогеев А. Г. Мониторинг и поддержка принятия решений в системе городского теплоснабжения на базе гетерогенной беспроводной сети / А. Г. Финогеев, В. А. Маслов, А. А. Финогеев, В. Е. Богатырев // Изв. ВолгГТУ. Серия. Актуальные проблемы управления, вычислительной техники и информатики в технических системах. – 2011. – Т. 3, № 10. – С. 73–81.

26. Финогеев А. Г. Анализ и классификация атак через беспроводные сенсорные сети в SCADA системах / А. Г. Финогеев, И. С. Нефедова, Е. А. Финогеев, Куанг Винь Тхай, П. В. Ботвинкин // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 1. – С. 12–23.

27. Финогеев А. Г., Финогеев А. А. Мобильные сенсорные сети для поддержки принятия решений / А. Г. Финогеев, А. А. Финогеев // ИНФО-2009 : сб. мат-лов Междунар. конф. (1–10 октября 2009 г.). – Сочи, 2009. – С. 146–-149.

28. Финогеев А. Г. Системы оперативного дистанционного контроля / А. Г. Финогеев, А. А. Финогеев // Надежность и качество : сб. трудов Междунар. симп. – Пенза : Изд. ПГУ, 2009. – Т. 2. – С. 124–126.

29. Чернобровцев А. Защита АСУ ТП / А. Чернобровцев // Computerworld Россия. – 2013. – № 10. – Режим доступа: http://www.osp.ru/news/articles/2013/37/13037680/ (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

30. Шахновский Г. Безопасность Систем SCADA и АСУТП / Г. Шахновский – Режим доступа: https://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/ (дата обращения 23.05.2014), свободный. – Заглавие с экрана. – Яз. рус.

31. Beitollahi H. A Cooperative Mechanism to Defense against Distributed Denial of Service Attacks / H. Beitollahi, G. Deconinck // The 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11), Changsha, China, November 16–18, 2011. – Changsha, 2011. – P. 11–20.

32. Beitollahi H. Analyzing Well-Known Countermeasures against Distributed Denial of Service Attacks / H. Beitollahi, G. Deconinck // Elsevier Journal of Computer Communications. – 2012.

33. Beitollahi H. Ferris Wheel: A Ring Based Onion Circuit for Hidden Services / H. Beitollahi, G. Deconinck // Elsevier Journal of Computer Communications. – 2012, April. – Vol. 35, issue 7. – P. 829–841.

34. Botvinkin P. V. Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems / P. V. Botvinkin, V. A. Kamaev, I. S. Nefedova, A. G. Finogeev, E. A. Finogeev // Life Science Journal. – 2014. – № 11 (11s). – P. 384–388.

35. IEEE (Institute of Electrical and Electronics Engineers) Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). Amendment 1: Add Alternate PHYs, 2007.

36. ISO 50001:2011 Energy management systems – Requirements with guidance for use. – 2011. – 22 p.

37. Rivest R. L. A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – New York, NY, USA: ACM, 1978. – Vol. 21. – № 2, Feb. – P. 120–126. – ISSN 0001-0782. – DOI:10.1.1.40.5588.

38. SCADA. Available at: http://en.wikipedia.org/w/index.php?title=SCADA&oldid =618278363 (accessed 23.05.2014).

39. Tyukov Anton. Digital signage based building energy management system: solution concept / Anton Tyukov, Andrey Ushakov, Maxim Shcherbakov, Adriaan Brebels, Valerij Kamaev // World Applied Sciences Journal. – Issue 24 (Information Technologies in Modern Industry, Education & Society). – P. 183–190.

40. Tyukov A. A concept of web-based energy data quality assurance and control system / A. Tyukov, A. Brebels, M. Shcherbakov, V. Kamaev // ACM International Conference Proceeding Series. – 2012. – P. 267–271.

41. ZigBee cluster library specification. – Available at: http://www.zigbee.org/zigbee/en/spec_download/spec_download.asp?AccessCode=1351395201 (accessed 04.06.2014).

42. ZigBee Specification Overview. – Available at: http://www.zigbee.org/Specifications/ZigBee/Overview.aspx (accessed 04.06.2014).

**References**

1. Bershadskiy A. M., Kurilov L. S., Finogeev A. G. Klassifikatsiya metodov marshrutizatsii v besprovodnykh sensornykh setyakh [Classification of methods for routing in wireless sensor networks]. *Izvestiya VolgGTU. Mezhvuzovskiy sbornik nauchnykh statey. Seriya. Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh* [News of VSTU. Interuniversity collection of scientific articles. Series. Actual problems of management, computer science and informatics in technical systems], 2012, vol. 10, no. 14, pp. 181–185.

2. Bershadskiy A. M., Kurilov L. S., Finogeev A. G. Obzor metodov marshrutizatsii v besprovodnykh sensornykh setyakh [Review of routing techniques in wireless sensor networks]. *Izvestiya VUZov. Povolzhskiy region. Tekhnicheskie nauki* [News of universities. Volga region. Technical sciences], 2012, no. 1, pp. 47–58.

3. Brays E. IT-bezopasnost v promyshlennosti. Glubokiy analiz paketov dannykh dlya SCADA-sistem [IT-security in industry. Deep packet data analysis for SCADA-systems]. Available at: http://issuu.com/cta-mag/docs/20134012 (accessed 23.05.2014).

4. Brumshteyn Yu. M., Podgornyy A. N. Informatsionnaya bezopasnost regiona: analiz soderzhaniya termina, modeley otsenki i nekotorykh voprosov upravleniya [Information security of the region: an analysis of the term, valuation models and some management issues]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: upravlenie, vychislitelnaya tekhnika i informatika* [Bulletin of the Astrakhan State Technical University. Series: Management, computer science and informatics], 2011, no. 1, pp. 24–29.

5. Brumshteyn Yu. M., Podgornyy A. N. Kompleksnyy analiz faktorov informatsionnoy i intellektualnoy bezopasnosti regionov [A comprehensive analysis of the factors of information and intellectual security of a regions]. *Informatsionnaya bezopasnost regionov* [Information security of regions], 2011, no. 1 (8), pp. 8–14.

6. Brumshteyn Yu. M., Tarkov D. A., Dyudikov I. A. Analiz modeley i metodov vybora optimalnykh sovokupnostey resheniy dlya zadach planirovaniya v usloviyakh resursnykh ogranicheniy i riskov [The models and methods analysis of optimum choice for decisions sets in conditions of resources restrictions and risks]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2013, no. 3 (23), pp. 169–180.

7. Varlataya S. K., Shakhanova M. V. Matematicheskie modeli dinamiki vozniknoveniya i realizatsii ugroz informacionnoy bezopasnosti [Mathematical models of the dynamics of the emergence and implementation of information security threats]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki* [Reports of Tomsk State University of Control Systems and Radio Electronics], 2012, no. 1–2, pp. 7–11.

8. Vorontsov A. A. Avtomatizirovannye sistemy upravleniya tekhnologicheskimi protsessami. Voprosy bezopasnosti [Automated process control systems. Security issues]. *JetInfo*, 2011, no. 5.

9. Gavrilov A. V. SCADA-sistemy [SCADA-systems]. Available at: http://www.insycom.ru /html/metodmat/Automat2011/Lect6.pdf (accessed 23.05.2014).

10. Gritsay G., Timorin A., Goltsev Yu., Ilin R., Gordeychik S., Karpin A. Bezopasnost promyshlennykh sistem v tsifrakh [Security of industrial systems in numbers]. Positive Technologies. Available at: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (accessed 23.05.2014).

11. Gusinskiy A. V., Kostrikin A. M., Voroshen V. A. et al. Informatsionno-izmeritelnye sistemy [Information-measuring systems], in 2 parts. Minsk, 2003, part 1. 40 p.

12. Zhabin S. A. Voprosy informatsionnoy bezopasnosti avtomatizirovannykh sistem kommercheskogo ucheta elektroenergii [Issues of information security of automated systems of commercial energy measuring]. *Algoritmy, metody i sistemy obrabotki dannykh* [Algorithms, methods, and systems for data processing], 2007, no. 12, pp. 75–80.

13. Zakharov D. A., Brumshteyn Yu. M. *Kompleksnoe primenenie informatsionno-kommunikatsionnykh tekhnologij v sfere telemeditsiny* [Integrated application of information and communication technologies in the field of telemedicine]. Astrakhan, Astrakhan State University, Publishing House "Astrakhan University", 2013. 133 p.

14. Kamaev V. A., Lezhebokov V. V. Razrabotka i primenenie modeli avtomatizirovannoy sistemy upravleniya informatsionnymi protsessami k zadache monitoringa sostojaniya oborudovaniya [Development and application of models of automated information management system to the task of monitoring the condition of the equipment]. *Vestnik kompyuternykh i informatsionnykh tekhnologiy* [Bulletin of Computer and Information Technologies], 2009, no. 9, pp. 18–22.

15. Kamaev V. A., Natrov V. V. Analiz metodov otsenki kachestva funktsionirovaniya i ehffektivnosti sistem zashhity informatsii na predpriyatiyakh elektroenergetiki [Analysis of methods to assess the quality of functioning and effectiveness of information security systems for energy companies]. *Izvestiya VolgGTU. Seriya. Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh* [News of VSTU. Interuniversity collection of scientific articles. Series. Actual problems of management, computer science and informatics in technical systems], 2007, issue 1, no. 1, pp. 67–69.

16. Kamaev V. A., Natrov V. V. Metodologiya obnaruzheniya vtorzheniy [Intrusion Detection Methodology]. *Izvestiya VolgGTU. Seriya. Konceptualnoe proektirovanie v obrazovanii, tekhnike i*

*tekhnologii* [News of VSTU. Series. Conceptual design in education, engineering and technology], 2006, issue 2, no. 2, pp. 127–132.

17. Kondakov V. V., Krasnoborodko A. A. *Informatsionnaya bezopasnost sistem fizicheskoy zashchity, ucheta i kontrolya yadernykh materialov* [Information security of systems of physical protection, accounting and control of nuclear materials]. Moscow, 2008. 48 p.

18. Methods to improve the reliability of SCADA systems. Available at: http://automation-system.ru/news/item/scada-2-2-2-2-2-2-2-2-2-2-2-2.html (accessed 23.05.2014). (In Russ.)

19. Mitreykin A. Nekotorye aspekty obespecheniya bezopasnosti ASU TP v TeK Rossii [Some aspects of safety of APCS in FEC of Russia]. *Informatsionnye resursy Rossii* [Information Resources of Russia], 2011, no. 4.

20. Pakhomov P. I., Nemtinov V. A. *Tekhnologiya podderzhki prinyatija resheniy po upravleniyu inzhenernymi kommunikatsiyami* [Technology for support decision-making in engineering communications management]. Moscow, Mashinostroenie, 2009. 124 p.

21. Supervisory control and data acquisition systems (SCADA-systems). Available at: http://www.mka.ru/?p=41524 (accessed 23.05.2014). (In Russ.)

22. Equipment for special services. Office for Scientific and Technical Information. Available at: http://www.bnti.ru/showart.asp?aid=792&lvl=04 (accessed 23.05.2014). (In Russ.)

23. Finogeev A. G., Dilman V. B., Maslov V. A., Finogeev A. A. Sistema udalennogo monitoringa i upravleniya setyami teplosnabzheniya na osnove besprovodnykh sensornykh setey [System for remote monitoring and control of district heating network based on wireless sensor networks]. *Prikladnaya informatika* [Applied Informatics],2011, no. 3 (33), pp. 83–93.

24. Finogeev A. G., Dilman V. B., Finogeev A. A., Maslov V. A. Operativnyy distantsionnyy monitoring v sisteme gorodskogo teplosnabzheniya na osnove besprovodnykh sensornykh setey [Operational remote monitoring in the urban heating system based on wireless sensor networks]. *Izvestiya VUZov. Povolzhskiy region. Tekhnicheskie nauki* [News of Universities. Volga region. Technical sciences], 2010, no. 3, pp. 27–36.

25. Finogeev A. G., Maslov V. A., Finogeev A. A. Bogatyrev V. E. Monitoring i podderzhka prinyatiya resheniy v sisteme gorodskogo teplosnabzheniya na baze geterogennoy besprovodnoy seti [Monitoring and support of decision-making in the urban heat based on heterogeneous wireless network]. *Izvestiya VolgGTU. Seriya. Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh* [News of VSTU. Interuniversity collection of scientific articles. Series. Actual problems of management, computer science and informatics in technical systems], 2011, vol. 3, no. 10, pp. 73–81.

26. Finogeev A. G., Nefedova I. S., Finogeev Ye. A., Kuang Vin Tkhay, Botvinkin P. V. Analiz i klassifikatsiya atak cherez besprovodnye sensornye seti v SCADA sistemakh [Analysis and classification of attacks via wireless sensor networks in SCADA systems]. Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii [Caspian Journal: Management and High Technologies], 2014, no. 1, pp. 12–23.

27. Finogeev A. G., Finogeev A. A. Mobilnye sensornye seti dlya podderzhki prinyatiya resheniy [Mobile sensor networks for support of decision making]. *INFO-2009: sbornik materialov Mezhdunarodnoy konferentsii* [INFO 2009: Proceedings of the International Conference], (1–10 October 2009). Sochi, 2009, pp. 146–149.

28. Finogeev A. G., Finogeev A. A. Sistemy operativnogo distantsionnogo kontrolya [Systems of operational remote control]. *Nadezhnost i kachestvo: sbornik trudov Mezhdunarodnogo simpoziuma* [Reliability and Quality: Proceedings of the International Symposium], 2009, vol. 2, pp. 124–126.

29. Chernobrovtsev A. Zashchita ASU TP [Protection of APCS]. Computerworld Rossiya. [Computerworld Russia], 2013, no. 10. Available at: http://www.osp.ru/news/articles/2013/37/13037680/ (accessed 23.05.2014). (In Russ.)

30. Shakhnovskiy G. Bezopasnost sistem SCADA i ASUTP [Security of SCADA-systems and APCS]. Available at: https://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/ (accessed 23.05.2014). (In Russ.)

31. Beitollahi H., Deconinck G. A Cooperative Mechanism to Defense against Distributed Denial of Service Attacks. *The 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11)*, Changsha, China, November 16–18, 2011. Changsha, 2011, pp. 11–20.

32. Beitollahi H., Deconinck G. Analyzing Well-Known Countermeasures against Distributed Denial of Service Attacks. *Elsevier Journal of Computer Communications*, 2012.

33. Beitollahi H., Deconinck G. Ferris Wheel: A Ring Based Onion Circuit for Hidden Services. *Elsevier Journal of Computer Communications*, 2012, April, vol. 35, issue 7, pp. 829–841

34. Botvinkin P. V., Kamaev V. A, Nefedova I. S, Finogeev A. G., Finogeev E. A. Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems. *Life Science Journal*, 2014, no. 11 (11s), pp. 384–388.

35. *IEEE (Institute of Electrical and Electronics Engineers) Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).* Amendment 1: Add Alternate PHYs, 2007.

36. ISO 50001:2011 Energy management systems – Requirements with guidance for use, 2011.

37. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. New York, NY, USA: ACM, 1978, vol. 21, no. 2, Feb. 1978, pp. 120–126. ISSN 0001-0782. DOI:10.1.1.40.5588/

38. SCADA. Available at: http://en.wikipedia.org/w/index.php?title=SCADA&oldid=618278363 (accessed 23.05.2014).

39. Tyukov Anton, Ushakov Andrey, Shcherbakov Maxim, Brebels Adriaan, Kamaev Valerij Digital signage based building energy management system: solution concept. *World Applied Sciences Journal*, issue 24 (Information Technologies in Modern Industry, Education & Society), pp. 183–190.

40. Tyukov A., Brebels A., Shcherbakov M., Kamaev V. A concept of web-based energy data quality assurance and control system. *ACM International Conference Proceeding Series*, 2012, pp. 267–271.

41. ZigBee cluster library specification. Available at: http://www.zigbee.org/zigbee /en/spec_download/spec_download.asp?AccessCode=1351395201 (accessed 04.06.2014).

42. ZigBee Specification Overview. Available at: http://www.zigbee.org/Specifications /ZigBee/Overview.aspx (accessed 04.06.2014).