УДК 002:004.056 + 342.7 Вестник УрФО № 2(28) / 2018, с. 60–70

Римша А. С., Югансон А. Н., Римша К. С.

ОБ ОДНОМ ПОДХОДЕ К ФОРМИРОВАНИЮ ПЕРЕЧНЯ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ ГАЗОДОБЫВАЮЩЕГО ПРЕДПРИЯТИЯ

Удаленное и географически распределенное расположение датчиков, промышленных контроллеров, приборов автоматики в АСУ ТП увеличивает риск вторжений и атак. В данной работе дана систематизация уязвимостей беспроводных сенсорных сетей АСУ ТП газодобывающего предприятия и атак, эксплуатирующих данные уязвимости. Предложена формула для вычисления коэффициента влияния отдельной уязвимости на величину потенциального ущерба. В заключении, сформулированы задачи, решение которых позволит спроектировать и построить защищенную беспроводную сенсорную сеть. Изложен общий подход к построению защищенной беспроводной сенсорной сети.

Ключевые слова: *беспроводные сенсорные сети, киберфизическая система, информационная безопасность АСУ ТП, оценка рисков.*

ON ONE APPROACH TO THE FORMATION OF A LIST OF MEASURES TO PROTECT INFORMATION IN WIRELESS SENSOR NETWORKS OF A GAS PRODUCING ENTERPRISE

Remote and geographically distributed location of sensors, industrial controllers, automation devices in the automated process control system increases the risk of intrusions and attacks. In this paper, a systematiztion of threats and vulnerabilities is made for wireless sensor networks of the automated process control system of a typical gas producing enterprise. A formula is for calculating the coefficient of influence of an individual vulnerability on the magnitude of potential damage. In conclusion, the tasks are formulated, the solution of which will allow to design and build a protected wireless sensor network. The general approach to building a secure wireless sensor network is outlined.

Keywords: *wireless sensor networks, cyber-physical system, SCADA information security, risk assessment.*

Введение

В настоящее время применение проводных систем при эксплуатации автоматизированных систем управления технологическими процессами (АСУ ТП) не всегда эффективно из-за высокой стоимости монтажных и пусконаладочных работ, а также технического обслуживания. Кроме того, в некоторых ситуациях установка проводных датчиков вообще невозможна по технологическим или организационным причинам. Достоинствами беспроводных датчиков являются минимальные ограничения по их размещению, возможность внедрения и модификации сети таких датчиков на эксплуатируемом объекте без вмешательства в процесс функционирования, надежность и отказоустойчивость всей системы в целом при нарушении отдельных соединений между узлами [1].

В свою очередь особое внимание уделяется беспроводным сенсорным сетям (БСС): самоорганизующейся сети множества датчиков и исполнительных устройств, объединенных между собой посредством радиоканала. Данная технология имеет множество преимуществ перед классическим проводным интерфейсом передачи данных: гибкая архитектура, снижение затрат при монтаже, высокие эксплуатационные параметры и другие [2].

Практическое использование беспроводных датчиков с автономным электропитанием долгое время сдерживалось низкой надежностью радиоканала по сравнению с проводным соединением, высокими стоимостью и энергопотреблением [3]. Сейчас, благодаря развитию элементной базы, миниатюризации интегральных микросхем и появлению новых технологий передачи информации, беспроводные датчики и основанные на них системы сбора данных и мониторинга стали реальностью и применяются во многих сферах деятельности человека [1].

Однако в связи с массовым внедрением киберфизических систем, и, как следствие, развитием рынка беспроводных устройств с одной стороны, и распространением промышленного шпионажа, распространением международного терроризма, увеличением количества техногенных аварий с другой стороны, обеспечение конфиденциальности ра-

диоканала, целостности передаваемой информации, доступности беспроводных устройств и каналов связи является одной из приоритетных задач при построении новых и совершенствовании существующих систем БСС.

Прежде всего, проведем обзор публикаций, охватывающих тематику "информационной безопасности беспроводных технологий". В работе [4] приведены принципы проектирования структуры сенсорной телекоммуникационной системы на базе технологии ZigBee оптимальной, по мнению авторов, для предприятий газотранспортной отрасли. Основной недостаток, с которым приходится сталкиваться при использовании беспроводных технологий - надежность таких сетей, которую можно повысить увеличением количества сенсоров. При этом авторы не рассматривают вопросы целостности, доступности и конфиденциальности информации, передаваемой от беспроводных модулей до центра управления. В работе [5] предложены методы резервирования и планирования приоритетов, алгоритмов маршрутизации и балансировки нагрузки для повышения надежности передачи технологических данных, что положительно сказывается на доступности БСС, но никак не на передаваемой в ней информации. Статья [6] содержит классификацию по типам и источникам угроз в беспроводных сетях на сигнальном и информационном уровне, однако вопросам резервирования и повышения отказоустойчивости беспроводных сетей должного внимания не было уделено.

Таким образом, задача классификации угроз уязвимостей БСС в типовом газодобывающем предприятии для топологии БСС mesh network (самоорганизующиеся сети) является актуальной.

Систематизировав уязвимости и атаки на БСС из указанных источников можно обозначить список мероприятий для защиты БСС от этих угроз.

Цель данной статьи – сформулировать перечень актуальных угроз и определить круг задач, решение которых позволит спроектировать защищенную БСС.

Описание структуры АСУ ТП газодобывающего предприятия

Типовое газодобывающее предприятие представляет собой территориально распределенную структуру, которая начинается от кустов газовых скважин и заканчивается центральным диспетчерским пунктом [7,8]. Как правило, в промышленных АСУ ТП выделяют три уровня:

– нижний уровень — уровень датчиков и исполнительных механизмов;

– средний уровень — уровень промышленных контроллеров;

– верхний уровень — система сбора данных и оперативного диспетчерского управления (англ., SCADA – Supervisory Control And Data Acquisition).

Анализ типовой архитектуры АСУ ТП позволяет выделить четыре зоны ответственности в плане реализации мероприятий безопасности беспроводных соединений:

1) транспортную зону сбора и передачи данных на основе беспроводной сенсорной сети, в которой узлы сенсорной сети объединены с датчиками, промышленными логическими контроллерами (ПЛК) и исполнительными механизмами, где выполняются производственные и технологические процессы [9];

2) зона беспроводной передача данных между серверами ввода/вывода (SCADA) и ПЛК, использующие подключение через радиомодем или устройство широкополосного доступа (УШПД);

3) интерфейсную зону диспетчерского контроля и управления, где работают операторы и диспетчеры с целью наблюдения за ходом выполнения технологического процесса [10,11];

4) зону выхода SCADA систем во внешнюю сеть для передачи данных в центральный офис (например, GSM связь).

Первая и вторая зоны ответственности являются предметом исследования. В этих зонах наиболее сложно реализовать традиционные меры обеспечения безопасности. Рассмотрим их подробнее.

Первая зона ответственности. Во-первых, производители датчиков, контроллеров и электронной компонентной базы разрабатывают собственные закрытые протоколы функционирования, которые не позволяют внедрить технологии защиты посредством IPSec, SSL и VPN и т. п. Во-вторых, довольно часто транспортная среда представляет собой пространственно-распределенные сети на большой территории. Такие сети характерны при реализации SCADA-систем городских инженерных коммуникаций [12] (сетей тепло-, водо-, электро- и газоснабжения), нефте- и газопроводов и т. п. Здесь для передачи данных и команд используются модемные соеди-

нения (GPRS,/3G) через существующие телефонные сети и сети операторов сотовой связи публичного доступа. Для функционирования сенсорных узлов им выделяются «серые» или «белые» IP-адреса в сети мобильного оператора, что фактически означает предоставление общедоступного канала для проведения внешних атак. В-третьих, при построении сети в рамках ограниченного пространства, контроллеры и исполнительные механизмы часто подключаются по последовательному интерфейсу (RS-232/RS-485) закрытой промышленной сети к MODBUS-серверу, или по беспроводной сенсорной сети к координатору. MODBUS-сервер и координатор, как правило, имеет шлюз для выхода в корпоративную сеть предприятия и далее в Интернет с поддержкой технологий удаленного доступа и управления по протоколам стека TCP/IP. Таким образом, обеспечивается доступ к данным и узлам SCADA-системы из корпоративной предприятия и диспетчерской зон и удаленный доступ из сети Интернет [13].

Вторая зона ответственности. На практике расстояние между технологическими установками, объединенными в одну систему управления, достигает нескольких километров, поэтому с точки зрения экономической эффективности (монтаж кабеля) и повышения надежности (обрыв кабеля) на удаленных объектах часто используются решения с применением беспроводного канала связи. В зависимости от расстояния между серверами ввода/вывода и ПЛК, а также наличия интерфейсов, используются подключение через радиомодем или устройство широкополосного доступа (УШПД). От радиомодема и УШПД сигнал приходит на радиомачту, от которой подключается к промышленному коммутатору. Помимо беспроводного подключения также могут использоваться волоконно-оптические линии, которые напрямую подключаются к коммутатору, но для повышения надежности приходится резервировать такие каналы связи, что увеличивает расходы. Одними из часто используемых шин передачи данных, используемых на производстве, являются Ethernet или специальная промышленная шина Profibus DP. Цифровая сеть позволяет объединить разнесенные компоненты системы в единый программно-аппаратный комплекс.

Сенсорные узлы могут включаться в общую инфраструктуру автоматически и спонтанно и размещаться на удаленных неохраняемых объектах, поэтому они могут быть захвачены и взломаны злоумышленником с целью использования их как источников атак. В сенсорных сетях немаловажное значение имеет своевременное обнаружение и изоляция таких скомпрометированных узлов, и активная защита от атак с их стороны до момента обнаружения. Критической угрозой для беспроводной сенсорной сети является внедрение через скомпрометированные узлы кодов для кражи важных данных о контролируемых процессах или для нарушения их корректной работы [13].

Постановка проблемы

Оценка уязвимости промышленной системы – это процесс выявления, анализа, классификации уязвимостей [14] с оценкой рисков безопасности и возможного ущерба при ее эксплуатации злоумышленниками или вредоносными программами [13].

При использовании беспроводной транспортной среды для передачи данных и команд достаточно просто перехватить и подменить кадры, передаваемые по сети, на кадры с вредоносным содержимым. Можно организовать генерацию и рассылку большого числа сторонних кадров в БСС, чтобы вызвать «отказ в обслуживании» (denial-of-service – DoS-атаку) промышленного оборудования или сетевого узла [15]. И, наконец, нарушить работу радиопередающих сетевых устройств можно путем генерации мощного электромагнитного излучения в частотном диапазоне БСС импульсного характера или сигнала типа «белый шум» (jamming attack) [13].

Выделим основные причины невысокой эффективности традиционных механизмов защиты передаваемых данных [16] для обеспечения безопасности SCADA-систем с беспроводными сенсорными сетями:

1) топология и динамические маршруты в сенсорной сети строятся на основе информации, полученной от координаторов, маршрутизаторов или оконечных сенсорных узлов по принципу «маршрутизация от источника» [1];

2) при работе алгоритмов маршрутизации используется механизм широковещательной рассылки маршрутных кадров и квитанций подтверждения. Широковещательная рассылка также используется при конфигурировании сети и поиске новых узлов;

3) после построения маршрута передача кадров осуществляется последовательно по цепочке между соседними узлами по одному

маршруту, который можно разрушить или изменить в любой момент времени;

4) идентификация сенсорных узлов и кадров данных осуществляется только на основе адресной информации, полученной сенсорными узлами от координатора сети, что позволяет подменить координатор и переназначить адреса;

5) аутентификация кадров данных и узлов сети в большинстве случаев просто не выполняется, что позволяет подменить сенсорные узлы и маршрутизаторы на «чужие» узлы с вредоносной «прошивкой». Широковещательная аутентификация узлов и кадров данных являются необходимым условием обеспечения защиты и устойчивости работы БСС [13].

Оценка рисков

Для примера возьмем множество всех беспроводных датчиков, используемых в технологическом процессе:

$C_{sensor} = \{c_0^{sensor}, \dots, c_5^{sensor}\}$, где $C_0 sensor$ - приемник, $C_1 sensor, \dots, C_5 sensor$ - беспроводные датчики.

В отличие от предложенной обобщённой математической модели АСУ ТП [17] для представления взаимодействия устройств друг с другом будет использоваться сетевая модель OSI, где каждому ее уровню (физическому, канальному, сетевому, транспортному, сеансовому, представления, прикладному) будет соответствовать матрица смежности, размерность которой определяется числом компонентов системы |C|, а в качестве значений будут указываться сетевые протоколы [18]. Таким образом, множество взаимодействий устройств будет представлено в следующем виде:

$$S = \{S^1, \dots, S^7\} \quad (1),$$

где , $S^k = \begin{vmatrix} 0 & \dots & s_{1j}^k & \dots & s_{1i}^k & \dots & s_{1n}^k \\ \dots & 0 & \dots & \dots & \dots & \dots & \dots \\ s_{j1}^k & \dots & 0 & \dots & s_{ji}^k & \dots & s_{jn}^k \\ \dots & \dots & \dots & 0 & \dots & \dots & \dots \\ s_{i1}^k & \dots & s_{ij}^k & \dots & 0 & \dots & s_{in}^k \\ \dots & \dots & \dots & \dots & \dots & 0 & \dots \\ s_{n1}^k & \dots & s_{nj}^k & \dots & s_{ni}^k & \dots & 0 \end{vmatrix}$

k – уровень модели OSI,

s_{ij} – протоколы взаимодействия.

Беспроводные сенсорные сети организуются на двух основных топологиях [1]:

1. Mesh network – самоорганизующиеся ячеистые сети (рис. 1).

2. Звезда – жестко заданная сеть (рис. 2).

Самоорганизующиеся ячеистые сети (Mesh network) образуются на основе множества соединений типа «точка–точка», находящихся в области радиопокрытия друг друга (рис. 1).

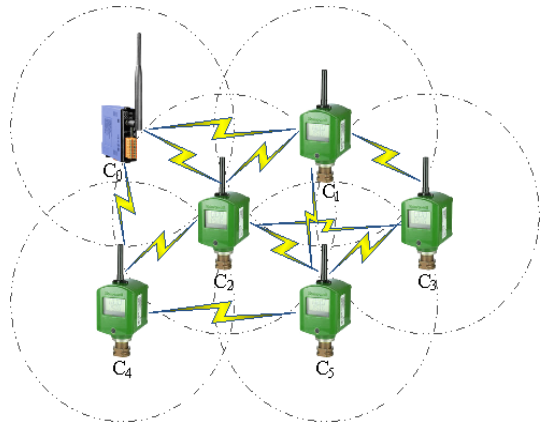

Рис. 1. Ячеистая топология самоорганизующейся сети

Такая технология позволяет беспроводным полевым приборам самостоятельно взаимодействовать друг с другом. Ключевыми преимуществами ячеистых сетей являются: автоматическое соединение между датчиками и способность любого датчика выполнять функции транзитной передачи данных для других участников сети. Сеть на основе ячеистой топологии надежна, обладает большой пропускной способностью. Высокая надежность обеспечивается наличием резервных маршрутов передачи данных: при выводе одного из датчиков из эксплуатации данные будут передаваться в обход по резервному пути, если этот датчик не являлся ключевым в этой ветке. Использование нескольких альтернативных маршрутов повышает пропускную способность сети. Снижение энергопотребления достигается снижением мощности сигналов посредством передачи данных через большее число узлов, разделенных меньшими расстояниями [17].

Топология «звезда» представляет собой централизованную систему, в которой каждое полевое устройство связывается с одной общей точкой доступа (шлюзом) напрямую. Каждый полевой прибор должен иметь прямую видимость со шлюзом, поэтому при добавлении нового устройства в сеть необходимо обеспечить прямую видимость как минимум с одной точкой доступа (рис. 2).

Далее рассмотрим влияние основных типов уязвимостей на активы БСС. Под актива-

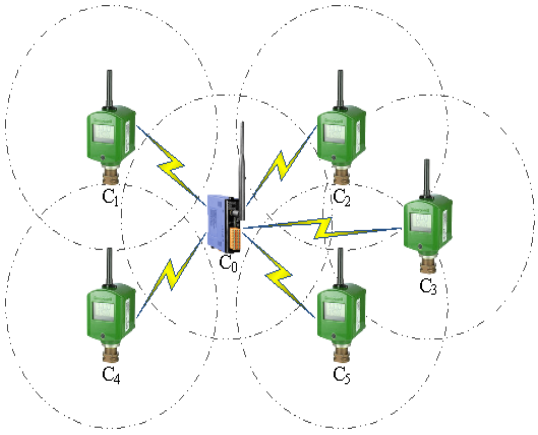

Рис. 2. Топология "звезда" для самоорганизующейся сети

ми будем рассматривать элементы беспроводной системы, под уязвимостями – условия реализации угрозы (табл. 1).

Количественное определение влияния конкретной уязвимости на определенный актив определяется экспертным путем на основе типовой модели угроз, разработанной для конкретного газодобывающего предприятия, использующего БСС в своей архитектуре АСУ ТП [19].

Влияние одной уязвимости на множество активов рассчитывается по следующей формуле:

$$V_j = \sum_{i=1}^{o} v_{ij} \times A_i \qquad (2)$$

При реализации угрозы нарушается технологический процесс, результатом которого может быть выход из строя компонентов системы [20]. Под ущербом, нанесенным в таком случае, будем понимать совокупность

Таблица 1

Матрица влияния уязвимостей на активы для беспроводных технологий

№ п/п	Уязвимости\Активы	Приемник	Передатчик	Антенны
Угрозы нарушения конфиденциальности				
1	Наличие в передаваемых данных отличительных признаков, работа на одном канале	v1,1	v1,2	v1,3
2	Использование стандартных форматов без дополнительной коррекции	v2,1	v2,2	v2,3
3	Отсутствие маскировки синхронизации и маркеров доступа	v3,1	v3,2	v3,3
4	Возможность сбора статистики передачи информации, использование при передаче открытых кодов	v4,1	v4,2	v4,3
5	Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала	v5,1	v5,2	v5,3
6	Наличие в каналах незашифрованной и расшифрованной информации	v6,1	v6,2	v6,3
7	Наличие аппаратуры на прием	v7,1	v7,2	v7,3
Угрозы нарушения целостности				
8	Наличие пересечений в сигнальных и логических областях команд и директив	v8,1	v8,2	v8,3
9	Неполная реализация протокола	v9,1	v9,2	v9,3
10	Низкая фильтрация сигналов основного канала	v10,1	v10,2	v10,3
11	Возможность определения протокола обмена	v11,1	v11,2	v11,3
12	Возможность выделения и определения идентификационных преамбул	v12,1	v12,2	v12,3
13	Наличие логического или физического адреса объекта воздействия	v13,1	v13,2	v13,3
Угрозы нарушения доступности				
14	Неполное тестирование аппаратуры	v14,1	v14,2	v14,3
15	Работа в условиях помех	v16,1	v16,2	v16,3
16	Наличие незакрепленных деталей	v17,1	v17,2	v17,3
17	Плохое экранирование приемной аппаратуры, побочные полосы	v18,1	v18,2	v18,3
18	Наличие отражающих поверхностей, низкое расположение антенн	v19,1	v19,2	v19,3

всех уязвимостей конкретной угрозы с учетом потенциального воздействия каждой.

Так как под ущербом мы подразумеваем реализацию угрозы, то оценка ущерба от конкретной угрозы будет определяться совокупностью уязвимостей, которые с ней связаны:

$$T_h = \sum_{j=1}^{m} t_{hj} \times V_j = \sum_{j=1}^{m} \left(t_{hj} \times \sum_{i=1}^{n} v_{ij} \times A_j \right) \quad (3)$$

Для оценки коэффициента влияния отдельной уязвимости на величину потенциального ущерба от угрозы с присутствием данной уязвимости воспользуемся следующей формулой [21]:

$$x = \frac{\sum_{i=1}^{n} P(t_i \mid c_1)}{\sum_{i=1}^{n} P(t_i)} \quad (4)$$

где $T = \{t_i\}$ – множество не взаимосвязанных угроз информационной безопасности с присутствием конкретной уязвимости;

$P(t_i)$ – вероятность возникновения любой угрозы из множества T;

$P(t_i|c_1)$ – вероятность возникновения угрозы с присутствием конкретного уязвимости.

Систематизация уязвимостей и атак на БСС

Под атакой будет понимать попытку получить несанкционированный доступ к сервису, ресурсу либо информации. Атакой также может быть попытка скомпрометировать целостность, доступность и конфиденциальность системы.

Существует огромное множество возможных атак на системы [22]. Например, некоторые атаки могут быть направлены на перехват сообщений, их изменение и дальнейшую отправку получателю для реализации более сложных атак, таких как создание зловредных узлов с целью организации ложных шлюзов. Опираясь на исследование [23] можно выделить две группы атак: активные и пассивные.

К пассивным атакам (П) относятся атаки, направленные на прослушивание траффика, аггрегирование и несанкционированный съем информации путем внедрения в коммуникационные протоколы или с помощью мониторинга сетевых пакетов. К активным атакам (А) можно отнести атаки, связанные с внедрением помех в БСС, представление вредоносного узла в качестве легитимного, изменение сетевых потоков и их источников, создание дыр в протоколах безопасности, нарушении производительности БСС и т.д.

Выявленных уязвимостей и наиболее значимые атаки на БСС типового газодобывающего предприятия можно систематизировать следующим образом:

Заключение

В результате проведенной систематизации уязвимостей и атак на БСС типового газодобывающего предприятия, был сформирован следующий перечень задач, решение которых позволит спроектировать и построить защищенную БСС:

1) должна быть обеспечена устойчивость к активным радиопомехам;

2) должно быть настроено автоматическое обнаружение и выявление подмененных узлов сенсорной сети;

3) должны быть созданы резервные маршруты передачи данных;

4) должно быть настроено автоматическое обнаружение и предотвращение попыток реконфигурирования сети, подмены адресной информации, несанкционированной «перепрошивки» устройств;

5) должны быть использованы механизмы идентификации и аутентификации узлов и кадров;

6) должна быть обеспечена устойчивость к искажению и фильтрации кадров данных;

7) должен быть применен механизмы канального шифрования кадров данных и управления ключами.

Таблица 2

Систематизация уязвимостей и атак на БСС

Уровень	Вид атаки	Эксплуатируемые уязвимости
Физический уровень	Создание радиотехнических помех (А)	Плохое экранирование приемной аппаратуры, побочные полосы
		Работа в условиях помех
		Наличие отражающих поверхностей, низкое расположение антенн
	Несанкционированный доступ (П)	Наличие в каналах незашифрованной и расшифрованной информации
		Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала
		Наличие аппаратуры на прием
		Возможность сбора статистики передачи информации, использование при передаче открытых кодов
Канальный уровень	Коллизия (А)	Работа в условиях помех
		Плохое экранирование приемной аппаратуры, побочные полосы
	Исчерпание энергоресурсов (А)	Возможность определения протокола обмена
		Низкая фильтрация сигналов основного канала
	Анализ трафика (П)	Возможность сбора статистики передачи информации, использование при передаче открытых кодов
		Возможность определения протокола обмена
Сетевой	Выборочная переадресация (А)	Отсутствие маскировки синхронизации и маркеров доступа
		Использование стандартных форматов без дополнительной коррекции
	Ошибочная адресация (А)	Наличие в передаваемых данных отличительных признаков, работа на одном канале
		Отсутствие маскировки синхронизации и маркеров доступа
		Плохое экранирование приемной аппаратуры, побочные полосы
	Репликация узлов (А)	Неполное тестирование аппаратуры
		Наличие логического или физического адреса объекта воздействия
		Возможность выделения и определения идентификационных преамбул
	Спуфинг, имитация соединения (П)	Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала
		Наличие в передаваемых данных отличительных признаков, работа на одном канале
Транспортный	Десинхронизация, рассогласование (А)	Неполная реализация протокола
	Флудинг, лавинная рассылка (А)	Наличие пересечений в сигнальных и логических областях команд и директив
		Наличие в передаваемых данных отличительных признаков, работа на одном канале
Прикладной	Определение местонахождения узла (А)	Наличие логического или физического адреса объекта воздействия
	Отказ в обслуживании (А)	Наличие пересечений в сигнальных и логических областях команд и директив
		Низкая фильтрация сигналов основного канала
		Возможность выделения и определения идентификационных преамбул
	Переполнение (А)	Неполная реализация протокола
		Неполное тестирование аппаратуры

Литература

1. Байтимиров А.Д., Шустрова М.Л. Беспроводные технологии в промышленности // Вестник Казанского технологического университета. 2014. — № 14. — С. 473–475.

2. Бушмелев П.Е., Увайсов С.У., Плюснин И.И., Бушмелева К.И. Беспроводная сенсорная сеть обнаружения утечек газа на магистральных газопроводах // Инновационные информационные технологии. Материалы международной научно-практической конференции, 2012. — С. 377-380.

3. Богданов С.П., Басов О.О. Перспективы и проблемы применения беспроводных датчиков с автономным питанием // Доклады ТУСУРа. 2012. — № 2 (26), ч. 1. — С. 231–238.

4. Барабанова Е.А., Мальцев Д.Б., Есауленко В.Н., Руденко М.Ф. Распределенная система контроля технологических объектов нефтегазовой промышленности на базе беспроводной сенсорной сети // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. — № 2. — С. 98–104.

5. Пикалов А.И., Галимов Р.Р. Анализ методов повышения отказоустойчивости беспроводной сети распределенных систем контроля и управления технологическими объектами // Приволжский научный вестник. 2016. — № 6 (58). — С. 23–27.

6. Карцан Р.В., Карцан И.Н. Беспроводной канал передачи информации, и ее защита // Актуальные проблемы авиации и космонавтики. 2015. — Т. 1. № 11. — С. 494–496.

7. Khan W.Z. Oil and Gas monitoring using Wireless Sensor Networks: Requirements, issues and challenges // Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 2016 International Conference on. — IEEE, 2016. — PP. 31-35.

8. Масагутов Р. АСУ ТП установки подготовки газа с расширенной функциональностью системы ПАЗ // Современные технологии автоматизации. 2012. — № 2. — С. 20–29.

9. Zhu C. A virtual grid-based real-time data collection algorithm for industrial wireless sensor networks // EURASIP Journal on Wireless Communications and Networking. 2018. — Vol. 2018. — № 1. — P. 134.

10. Taboun M.S., Brennan R.W. An Embedded Multi-Agent Systems Based Industrial Wireless Sensor Network // Sensors. 2017. — Vol. 17. — №. 9. — P. 2112.

11. Taboun M.S., Brennan R.W. An Embedded Agent-Based Intelligent Industrial Wireless Sensor Network // International Conference on Industrial Applications of Holonic and Multi-Agent Systems. — Springer, Cham, 2017. — PP. 227-239.

12. Синещук М.Ю. Особенности обеспечения информационной безопасности АСУ ТП потенциально опасных объектов // Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций. 2015. — № 1 (6). — С. 49–51.

13. Финогеев А.Г., Нефедова И.С., Тхай К.В. Проблемы безопасности беспроводной сенсорной сети в SCADA-системах АСУ ТП // Известия ВолгГТУ. 2014. — № 6 (133). — С. 66–72.

14. Shcherbakov M.V., Brebels A., Shcherbakova N.L., Tyukov A.P., Janovsky T.A., Kamaev V.A. A Survey of Forecast Error Measures // World Applied Sciences Journal (WASJ). 2013. — Vol. 24, Spec. Issue 24: Information Technologies in Modern Industry, Education & Society. — PP. 171–176.

15. Агафонов А.В., Синадский Н.И. Структура и принцип работы комплекса тестирования устойчивости телекоммуникационного оборудования к сетевым атакам типа «отказ в обслуживании» // Вестник УрФО. Безопасность в информационной сфере. 2015. — № 4 (18). — С. 4–11.

16. Финогеев А.Г., Нефедова И.С., Тхай Куанг Винь. Проблемы безопасности беспроводной сенсорной сети в SCADA-системах АСУ ТП // Известия ВолгГТУ. 2014. — № 6 (133). — С. 66–72.

17. Захаров А.А., Римша А.С., Харченко А.М., Зулькарнеев И.Р. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия // Вестник УрФО. Безопасность в информационной сфере. 2017. — № 3 (25). — С. 24–33.

18. Cao N. The Comparisons of Different Location-Based Routing Protocols in Wireless Sensor Networks // Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on. – IEEE, 2017. — Vol. 2. — PP. 324-327.

19. Taylor J.H. Intelligent control and asset management: An event-based control road map // Paper presented at the 2016 2nd International Conference on Event-Based Control, Communication, and Signal Processing. EBCCSP 2016 — Proceedings, doi:10.1109/EBCCSP.2016.7605269

20. Римша А.С. К вопросу об информационной безопасности автоматизированных систем управления технологическими процессами газодобывающего предприятия // Сборник тезисов докладов: Вторая Арктическая совместная науч.-практ. конф., Новый Уренгой, 16-19 мая 2018 / ООО «Газпром добыча Уренгой» и «Газпром добыча Ямбург», 2018. — С. 84-85.

21. Дерендяев Д.А., Гатчин Ю.А., Безруков В.А. Математическая модель оценки коэффициента вли-

яния отдельно взятого фактора на угрозы информационной безопасности // Кибернетика и программирование. 2016. — № 5. — С. 83–88.

22. Chhaya L. Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control // Electronics. — 2017. — Vol. 6. — № 1. — P. 5.

23. Mohammadi S., Jadidoleslamy H.A comparison of link layer attacks on wireless sensor networks. // International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks. 2011. — № 3 (1), PP. 69–84.

References

1. Baitimirov A.D., Shustrova M.L. Wireless Technologies in Industry [Besprovodnye tekhnologii v promyshlennosti] // Vestnik Kazanskogo tekhnologicheskogo universiteta. 2014. — № 14. — PP. 473–475.

2. Bushmelev P., Uvaysov S., Plusnin I., Bushmeleva K. Wireless sensor network detection of leaks on the main gas pipelines [Besprovodnaya sensornaya set obnaruzheniyautechek gaza na magistralnykh gazoprovodakh] // Innovative information technologies. Materials of the International Scientific and Practical Conference, 2012. — PP. 377-380.

3. Bogdanov S.P., Basov O.O. Prospects and Problems of Using Wireless Sensors with Autonomous Power Supply [Perspektivy i problemy primeneniia besprovodnykh datchikov s avtonomnym pitaniem] // Doklady TUSURa. 2012. — № 2 (26), ch. 1. — PP. 231–238.

4. Barabanova E.A., Maltsev D.B., Esaulenko V.N., Rudenko M.F. Distributed Control System for Technological Objects of Oil and Gas Industry on the Basis of Wireless Sensor Network [Raspredelennaia sistema kontrolia tekhnologicheskikh obieektov neftegazovoi promyshlennosti na baze besprovodnoi sensornoi seti] // Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitelnaia tekhnika i informatika. 2017. — № 2. — PP. 98–104.

5. Pikalov A.I., Galimov R.R. Analysis of Methods for Increasing the Fault Tolerance of a Wireless Network of Distributed Monitoring and Control Systems for Technological Objects [Analiz metodov povysheniia otkazoustoichivosti besprovodnoi seti raspredelennykh sistem kontrolia i upravleniia tekhnologicheskimi obieektami] // Privolzhskii nauchnyi vestnik. 2016. — № 6 (58). — PP. 23–27.

6. Kartsan R.V., Kartsan I.N. Wireless Channel of Information Transmission and its Protection [Besprovodnoi kanal peredachi informatsii, i ee zashchita] // Aktualnye problemy aviatsii i kosmonavtiki. 2015. — Vol. 1. № 11. — PP. 494–496.

7. Khan W.Z. Oil and Gas monitoring using Wireless Sensor Networks: Requirements, issues and challenges // Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 2016 International Conference on. — IEEE, 2016. — PP. 31-35.

8. Masagutov R. APCS of the Gas Preparation Unit with Extended Functionality of the PA System [ASU TP ustanovki podgotovki gaza s rasshirennoi funktsionalnostiu sistemy PAZ] // Sovremennye tekhnologii avtomatizatsii. 2012. — № 2. — PP. 20–29.

9. Zhu C. A virtual grid-based real-time data collection algorithm for industrial wireless sensor networks // EURASIP Journal on Wireless Communications and Networking. 2018. — Vol. 2018. — № 1. — P. 134.

10. Taboun M.S., Brennan R.W. An Embedded Multi-Agent Systems Based Industrial Wireless Sensor Network // Sensors. 2017. — Vol. 17. — №. 9. — P. 2112.

11. Taboun M.S., Brennan R.W. An Embedded Agent-Based Intelligent Industrial Wireless Sensor Network // International Conference on Industrial Applications of Holonic and Multi-Agent Systems. — Springer, Cham, 2017. — PP. 227-239.

12. Sineshchuk M.I. Features of Ensuring Information Security of Automated Process Control Systems of Potentially Dangerous Objects [Osobennosti obespecheniia informatsionnoi bezopasnosti ASU TP potentsialno opasnykh obieektov] // Sovremennye tekhnologii obespecheniia grazhdanskoi oborony i likvidatsii posledstvii chrezvychainykh situatsii. 2015. — № 1 (6). — PP. 49–51.

13. Finogeev A.G., Nefedova I.S., Tkhai K.V. Security Problems of a Wireless Sensor Network in SCADA Systems of Automated Process Control Systems [Problemy bezopasnosti besprovodnoi sensornoi seti v SCADA-sistemakh ASU TP] // Izvestiia VolgGTU. 2014. — № 6 (133). — PP. 66–72.

14. Shcherbakov M.V., Brebels A., Shcherbakova N.L., Tyukov A.P., Janovsky T.A., Kamaev V.A. A Survey of Forecast Error Measures // World Applied Sciences Journal (WASJ). 2013. — Vol. 24, Spec. Issue 24: Information Technologies in Modern Industry, Education & Society. — PP. 171–176.

15. Agafonov A., Sinadsky N. Structure and operation principle of the hardware and software complex intended for testing the immunity of telecommunication equipment against denial of service network attacks [Struktura i printsip raboty kompleksa testirovaniya ustoychivosti telekommunikatsionnogo oborudovaniya k setevym atakam tipa «otkaz v obsluzhivanii»] // Vestnik UrFO. Bezopasnost v informatsionnoi sfere. 2015. — № 4 (18). — PP. 4–11.

16. Finogeev A.G., Nefedova I.S., Tkhai Kuang Vin. Security Problems of a Wireless Sensor Network in SCADA Systems of Automated Process Control Systems [Problemy bezopasnosti besprovodnoi sensornoi seti v SCADA-sistemakh ASU TP] // Izvestiia VolgGTU. 2014. — № 6 (133). — PP. 66–72.

17. Zakharov A.A., Rimsha A.S., Kharchenko A.M., Zulkarneev I.R. Analysis of Information Security of Automated Control Systems for Technical Processes of a Gas Producing Enterprise [Analiz informatsionnoi bezopasnosti avtomatizirovannykh sistem upravleniia tekhnicheskimi protsessami gazodobyvaiushchego predpriiatiia] // Vestnik UrFO. Bezopasnost v informatsionnoi sfere. 2017. — № 3 (25). — PP. 24–33.

18. Cao N. The Comparisons of Different Location-Based Routing Protocols in Wireless Sensor Networks // Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on. – IEEE, 2017. — Vol. 2. — PP. 324-327.

19. Taylor J.H. Intelligent control and asset management: An event-based control road map // Paper presented at the 2016 2nd International Conference on Event-Based Control, Communication, and Signal Processing. EBCCSP 2016 — Proceedings, doi:10.1109/EBCCSP.2016.7605269

20. Rimsha A.S. The problem of information security of automated control systems for technical processes of a gas producing enterprise [K voprosu ob informatsionnoy bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami gazodobyvayushchego predpriyatiya] // Proceedings of the Second Arctic joint scientific-practical conference, 2018. — PP. 84-85.

21. Derendiaev D.A., Gatchin I.A., Bezrukov V.A. A Mathematical Model for Estimating the Coefficient of Influence of an Individual Factor on Threats to Information Security [Matematicheskaia model otsenki koeffitsienta vliianiia otdelno vziatogo faktora na ugrozy informatsionnoi bezopasnosti] // Kibernetika i programmirovanie. 2016. — № 5. — PP. 83–88.

22. Chhaya L. Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control // Electronics. — 2017. — Vol. 6. — № 1. — P. 5.

23. Mohammadi S., Jadidoleslamy H. A comparison of link layer attacks on wireless sensor networks. // International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks. 2011. — № 3 (1). — PP. 69–84.

РИМША Андрей Сергеевич, аспирант кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: RimshaAndrew@gmail.com

Югансон Андрей Николаевич, аспирант кафедры проектирования и безопасности компьютерных систем. Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 197101, г. Санкт-Петербург. Кронверкский пр., 49. E-mail: a_yougunson@corp.ifmo.ru

Римша Константин Сергеевич, студент кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: RimshaKonstantin@ya.ru

RIMSHA Andrew, post-graduate student of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: RimshaAndrew@gmail.com

IUGANSON Andrei, post-graduate student of the Department of Computer System Design and Security. ITMO University. Bld. 49, Kronverksky avenue, Saint-Petersburg, 197101. E-mail: a_yougunson@corp.ifmo.ru

RIMSHA Constantin, student of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: RimshaKonstantin@ya.ru