СИСТЕМНЫЙ АНАЛИЗ, МОДЕЛИ И МЕТОДЫ ПРИНЯТИЯ РЕШЕНИЙ, УПРАВЛЕНИЕ В ЧЕТКИХ И НЕЧЕТКИХ УСЛОВИЯХ

УДК 621.391

АНАЛИЗ И КЛАССИФИКАЦИЯ АТАК ЧЕРЕЗ БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ В SCADA СИСТЕМАХ[1]

Статья поступила в редакцию 14.01.2014, в окончательном варианте 06.02.2014.

Финогеев Алексей Германович, доктор технических наук, профессор, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40, e-mail: finogeev@sura.ru

Нефедова Ирина Сергеевна, аспирант, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40, e-mail: nefedya2008@yandex.ru

Финогеев Егор Алексеевич, аспирант, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40, e-mail: nefedya2008@yandex.ru

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

Ботвинкин Павел Викторович, аспирант, Волгоградский государственный технический университет, 400123, Российская Федерация, г. Волгоград, ул. Коммунаров, д. 13, e-mail: pavel.botvinkin@gmail.com

Эффективность обеспечения информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), а также систем диспетчерского контроля и управления (SCADA – supervisory control and data acquisition systems) зависит от применяемых технологий защиты компонентов транспортной среды передачи данных. В статье исследуются проблемы обнаружения атак на беспроводные сенсорные сети (WSN – wireless sensor networks) SCADA систем. В результате аналитических исследований авторами разработана подробная классификация внешних атак на сенсорные сети и приведено подробное описание атакующих воздействий на компоненты SCADA системы в соответствии с выбранными направлениями атак. Рассмотрены способы обнаружения атак в беспроводных сенсорных сетях SCADA систем и функции системы беспроводного обнаружения вторжений (WIDS – wireless intrusion detection system). Отмечена роль фактора внутренних антропогенных угроз безопасности.

Ключевые слова: информационная безопасность, SCADA система, беспроводная сенсорная сеть, WSN, сетевые атаки, обнаружение сетевых атак, система обнаружения вторжений, WIDS, антропогенные угрозы безопасности

ANALYSIS AND CLASSIFICATION OF ATTACKS VIA WIRELESS SENSOR NETWORKS IN SCADA SYSTEMS

Finogeev Aleksey G., D.Sc. (Engineering), Professor, Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation, e-mail: finogeev@sura.ru

Nefedova Irina S., post-graduate student, Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation, e-mail: nefedya2008@yandex.ru

Finogeev Yegor A., post-graduate student, Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation, e-mail: nefedya2008@yandex.ru

[1] Работа выполнена при финансовой поддержке со стороны Минобрнауки России в рамках базовой части проекта 2586 задания № 2014/16.

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

Botvinkin Pavel V., post-graduate student, Volgograd State Technical University, 13 Kommunary St., Volgograd, 400123, Russian Federation, e-mail: pavel.botvinkin@gmail.com

Effectiveness of information security systems of automated process control systems (APCS) and supervisory control and data acquisition systems (SCADA) depends on applied technologies to protect components of the transport environment for data transfer. This article investigates the problem of detecting attacks on wireless sensor networks (WSN) of SCADA systems. As a result of analysis, authors developed detailed classification of external attacks on sensor networks and the detailed description of the attackers impacts on components of SCADA systems in accordance with the selected lines of attacks. Considered the methods of intrusion detection in wireless sensor networks SCADA systems and functions of the wireless intrusion detection system (WIDS). Noted the role of anthropogenic factors of internal security threats.

Keywords: Computer Security, SCADA, wireless sensor network, WSN, network attacks, detection of network attacks, intrusion detection system, WIDS, Anthropogenic threats to security

Введение. Эффективность решения задач по обеспечению информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) и систем диспетчерского контроля и управления (SCADA) в значительной степени зависит от применяемых технологий и средств защиты компонентов транспортной среды передачи данных.

Еще одним потенциально важным, но пока слаборазвитым 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 [4].

В связи с переходом на беспроводные сетевые технологии для построения сенсорных сетей сбора телеметрической информации, качество такой защиты [5], в свою очередь, определяется не только программно-аппаратными решениями промышленных контроллеров и сенсорных узлов, но и выбранными принципами их информационного взаимодействия в процессе синтеза топологии сети, определения маршрутов и передачи данных.

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. Также в ряде случаев накладываются довольно жесткие требования к временны*м* задержкам при обработке и передаче информации в транспортной среде, что вызвано необходимостью мониторинга и управления технологическими процессами в режиме реального времени [3, 10]. 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.

Если SCADA система разворачивается на большой территории, например, для мониторинга и управления распределенными инженерными сетями (тепло-, водо-, электро- и га-

зоснабжения) [8, 11], то в качестве передающей транспортной среды часто используется сеть операторов сотовой связи (модемные соединения GPRS/3G) с возможностью публичного доступа. Это фактически обеспечивает канал для проведения атак.

Поэтому для построения эффективных средств защиты информации в беспроводных сенсорных сетях необходимо проанализировать возможные типы атак; способы их обнаружения; причины уязвимостей систем. Решение этих задач и было целью настоящей работы.

Классификация видов атак в беспроводных сенсорных сетях. Используемые сейчас принципы передачи данных в беспроводных сетях обеспечивают возможность совершения четырёх видов воздействий: перехват, изменение, разрушение и инъекция кода. В соответствии с определением безопасности все атаки на беспроводные сенсорные сети (WSN) SCADA систем можно разделить по следующим категориям (рис. 1).

Рис. 1. Основные классы атак на WSN

1. Атаки доступа, к которым относятся попытки получить несанкционированный доступ к ресурсам системы.

2. Атаки на конфиденциальность, которые представляют собой попытки перехвата данных в транспортной среде передачи.

3. Атаки на целостность, которые включают генерацию и пересылку кадров для захвата контроля и управления над SCADA системой, для вызова сбоев и отказов в ее работе или для подготовки других атак.

Рассмотрим более детально классификацию атак по направлению воздействий и приведем подробное описание их основных видов (рис. 2).

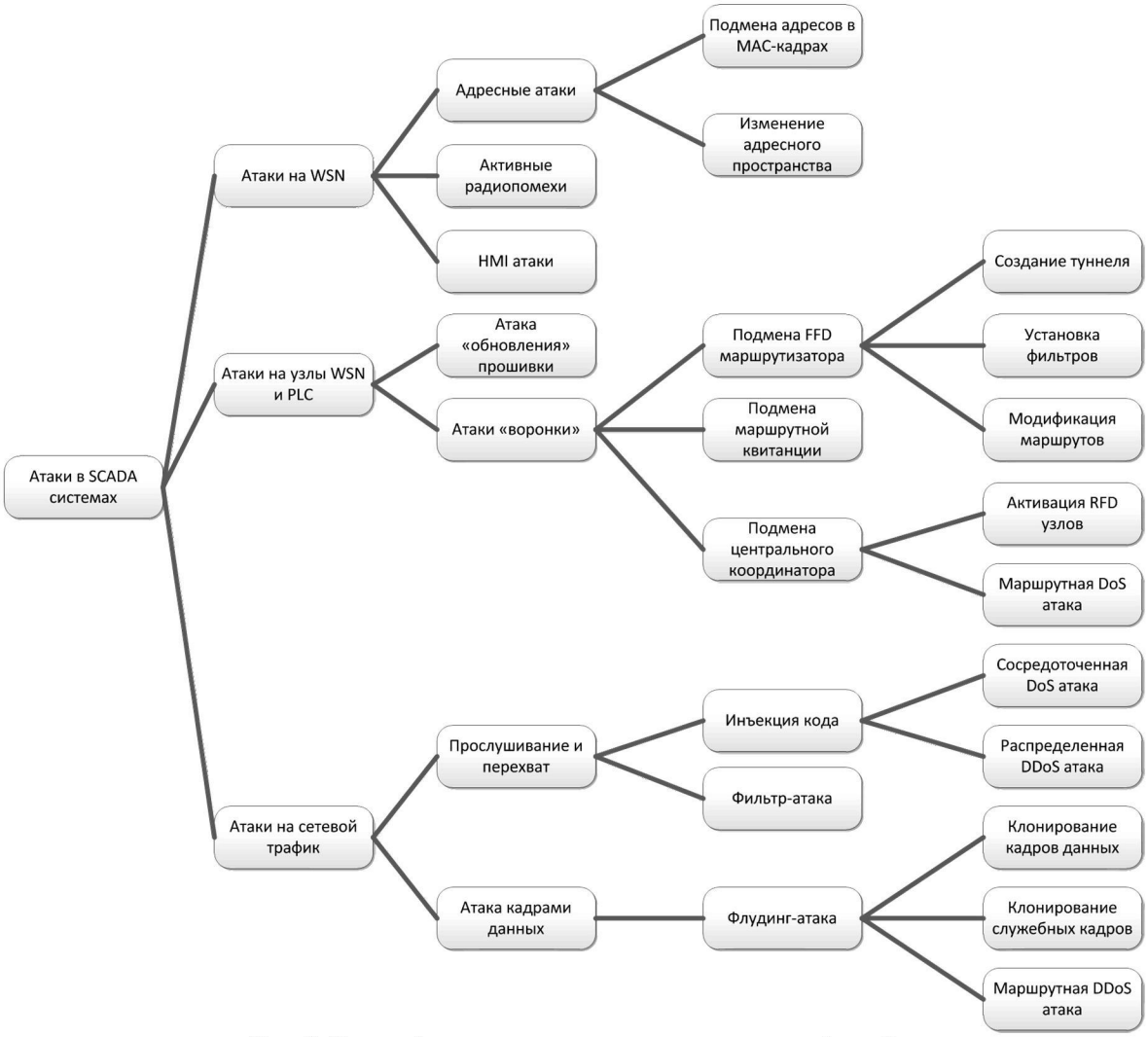

Рис. 2. Классификация атак по направлениям воздействий

А) Атаки на сенсорную сеть SCADA системы в целом.

А1) Создание активных радиопомех в зоне работы SCADA системы. Для создания постоянных помех используются генераторы «белого шума», работающие в той же полосе частот, что и SCADA системы. Источник постоянных помех можно определить с помощью спектральных анализаторов и прекратить атаку путем локализации и устранения источника [7]. Наиболее опасны естественные (молнии) или искусственные импульсные помехи, которые могут привести не только к сбою системы, но также к повреждению сенсорных узлов и промышленных контроллеров (PLC).

А2) Атаки на человеко-машинный интерфейс (HMI) SCADA системы [15]. Несанкционированный доступ к Web-интерфейсу диспетчера с мобильного устройства может осуществляться в случае использования открытых беспроводных сетей или сетей со слабой системой аутентификации.

А3) Атака с целью изменения адресов WSN (spoofing), направленная на инициирование «отказа в обслуживании» (Denial of Service – DoS). Можно выделить два вида такой атаки:

a) перехват кадров сенсорных узлов с целью подмены MAC адресов источников и приемников, что приводит к отказам и сбоям в работе SCADA системы;

b) подмена центрального координатора с целью изменения адресного пространства в конфигурации сенсорной сети. Для инициализации и поддержания работы сенсорной сети координатор периодически рассылает кадры опроса и кадры с назначенными сетевыми адресами. Если внедрить в расположении сенсорной сети другой координатор и подменить широковещательные кадры, то можно переназначить адреса оконечным устройствам и сконфигурировать новую сенсорную сеть. Далее можно использовать эту новую сеть для нарушения работы алгоритмов маршрутизации, для DoS атаки, для сбора данных через координатор, для передачи команд исполнительным механизмам.

Б) Атака на узлы сенсорной сети и связанные с ними устройства.

Б1) Изменение прошивок, драйверов и программного обеспечения (ПО) промышленных контроллеров (PLC) и оконечных сенсорных узлов (RFD – Reduced Function Device). Атака ведется путем сканирования PLC и сенсорных узлов для определения возможностей изменения предустановленной операционной системы (ОС), т.е. прошивки, драйверов и ПО контроллеров. Алгоритм такой атаки может включать следующие шаги. Сначала определяется достижимость конкретного узла (операция ping) в момент времени, когда он находится в активном режиме (для энергосбережения в системах обычно используется «спящий» режим работы узлов). Далее отправляется запрос о прошивке узла, ее версии и драйверах. Как правило, обновление прошивок, драйверов и прикладного ПО является базовым сервисом и выполняется автоматически в удаленном режиме. Поэтому на следующем этапе злоумышленник с root-правами доступа активирует процесс обновления и изменения прошивки, драйвера или ПО с инъекцией вредоносного кода.

Б2) Внедрение и/или подмена узлов WSN («атака воронки»). Основная цель такой атаки – перенаправление сетевого трафика на внедренный или замененный узел. Производится путем подмены узлов, ответственных за сбор и ретрансляцию данных в сети (FFD – Fully Function Device) с целью перехвата и перенаправления сетевого трафика. Изменения в работе протоколов маршрутизации вызывают перенаправление сетевого трафика по специально созданным маршрутам на внедренные узлы и препятствуют передаче данных с оконечных узлов (RFD) на пульты диспетчерского управления, что создает угрозу для работы SCADA системы. Кроме того, злоумышленник фактически получает полный контроль над исполнительными устройствами и доступ к интересующей зоне сети. Рассмотрим разновидности такой атаки:

a) компрометация узла сбора данных путем подмены квитанций подтверждения маршрутов для перенаправления трафика с оконечных узлов-источников на внедренный узел-приемник. В больших WSN, использующих спецификацию ZigBee Pro Feature Set, работают два способа маршрутизации сообщений: «маршрутизация от источника» (Source Routing) и «Многие-к-одному» (Many-to-One) [2]. Способ маршрутизации от источника (Source Routing) предполагает, что маршруты в сети хранятся на узлах-источниках, а для их определения все узлы рассылают периодически широковещательные запросы к узлам сбора данных, что перегружает сеть избыточным служебным трафиком. Кроме того, в этом случае для повышения надежности работает механизм квитирования, когда перед непосредственной передачей кадра данных каждый узел-источник широковещательно рассылает приемникам информацию о маршруте (пакет Route Record) и ждет квитанцию подтверждения о готовности приема данных конкретным устройством. Только после получения ответной квитанции посылается кадр данных. Если узел-источник не получает квитанции, то считается, что маршрут недоступен и производится широковещательный поиск нового маршрута. Внедренный в рамках атаки на сеть узел постоянно генерирует и рассылает квитанции подтвер-

ждения с адресом реального узла сбора, что увеличивает вероятность получения данной квитанции узлами-источниками раньше квитанции от реального координатора сети и, как следствие, последующей передачи кадра данных на внедренный узел. Так как объем доступной оперативной памяти у RFD узлов небольшой, то они могут помнить только лимитированное количество маршрутов, по которым ранее передавали данные в течение ограниченного времени после получения квитанций (возраст маршрута). Поэтому получение «ложной» квитанции в момент после «забывания» старого маршрута не вызывает у RFD устройства действий по проверке маршрутной информации и узел передает кадры по новому маршруту. В результате такой подмены реальный координатор прекращает сбор данных с PLC и датчиков и диспетчерская служба теряет контроль над технологическими процессами;

b) подмена маршрутизатора (FFD узла) в сенсорной сети для нарушения корректной работы алгоритмов маршрутизации. Атака может выполняться путем:

- создания «ложного» туннеля. На внедренном маршрутизаторе работает программа копирования ретранслируемых кадров с целью передачи в другую сенсорную сеть или, наоборот, программа передачи кадров с командами управления из другой сети;
- установки фильтров. На внедренном маршрутизаторе работает программа фильтрации и уничтожения ретранслируемых кадров по заданным критериям или по содержимому;
- изменения маршрутов. На внедренном маршрутизаторе работает программа, которая изменяет содержимое пакетов Route Record по заданному алгоритму либо случайным образом;

c) подмена центрального координатора WSN для организации широковещательного шторма и достижения «отказа в обслуживании». Основные цели такой подмены:

- генерация широковещательных кадров перевода оконечных сенсорных узлов в «активный» режим вне расписания для быстрой разрядки источников питания и т.д.;
- генерация широковещательных маршрутных кадров (маршрутная DoS атака). Атака возможна при использовании в WSN второго способа маршрутизации Many-to-One, который используется для снижения загрузки сети служебным трафиком. Согласно данному методу маршрутизации рассылка маршрутов производится от центрального узла-координатора, являющегося инициатором сбора данных и изменения маршрутной информации, к удаленным узлам [1]. Таким образом, рассылка «ложной» маршрутной информации приводит либо к отказам сети, либо к перенаправлению потоков данных на шлюз злоумышленника.

B) Атаки на сетевой трафик сенсорной сети.

B1) Прослушивание каналов передачи данных. Производится путем перехвата и декодирования сетевого трафика с помощью утилит-снифферов для последующего анализа кадров на предмет извлечения требуемой информации.

B2) Атаки кадрами данных. Выполняются путем флудинга или генерации «ложных» кадров (служебных или кадров данных) или замены содержимого перехваченных кадров и последующем внедрении в сеть. Рассмотрим основные варианты таких атак:

a) инъекция вредоносного кода. Используя уязвимости в работе сенсорных узлов, такие как, например, вероятность переполнения буфера, злоумышленник может отправить множество кадров (сосредоточенная DoS атака), чтобы осуществить переполнение стека и вызвать «отказ в обслуживании». При инъекции вредоносного кода производится его запуск на исполнение для вывода из строя исполнительных механизмов, всей сети в целом или изменения параметров контролируемых технологических процессов. Инъекция в маршрутизаторы сети самовоспроизводящегося червя приводит к заражению всех узлов и превращению этой сети в BotNet-сеть, узлы которой генерируют кадры данных с целью увеличения времени реакции сети, достижения сбоев и отказов (распределенная DoS атака [12, 13]);

b) фильтрация кадров и выборочная пересылка. Производятся путем внедрения в сеть специальных программных или аппаратных фильтров, которые задерживают кадры данных, фильтруют их, производят выборочную рассылку. При данной атаке можно отменить пересылку определённых кадров данных координатору сети, например, кадров, оповещающих о нештатных и аварийных ситуациях на объектах мониторинга, что не позволит диспетчерам принять своевременные меры и может вызвать катастрофические последствия. Эффективность атаки повышается при ее интеграции с атакой воронки;

c) флудинг-атаки путем генерации «ложных» кадров (служебных или кадров данных) и широковещательной рассылки:

- клонирование и широковещательная рассылка кадров данных. Выполняются путем перехвата и многократного воспроизведения одних и тех же кадров данных с последующей широковещательной рассылкой в сети для переполнения входных буферов и отказа сети;
- генерация и широковещательная рассылка кадров опроса узлов и кадров HELLO с целью достижения отказов сетевых ресурсов. Создавая и рассылая в сети множество HELLO-кадров с адресами несуществующих узлов, можно создать образ «несуществующей» зоны сенсорной сети;
- синтез «виртуальных» узлов-источников с целью широковещательной рассылки от них маршрутных пакетов (маршрутная DDoS атака). Здесь эксплуатируется недостаток технологии Source-Routing при использовании в централизованных SCADA системах с одним координатором и шлюзом, а именно – чрезмерная загрузка сети широковещательным маршрутным трафиком. После компрометации сенсорной сети и получения ключей доступа к ней производится сканирование и сбор кадров Route Record для извлечения данных о MAC-адресах сетевых узлов. Далее в процессе атаки узел-нарушитель генерирует множество пакетов Route Record с виртуальными адресами источников и широковещательно рассылает их для нарушения нормального процесса маршрутизации, что приводит к отказам в работе сети и SCADA системы.

Обнаружение атак в беспроводных сенсорных сетях SCADA систем. В общем случае существуют традиционные приемы выявления атак в транспортной сетевой среде [6, 14], которые включают следующие процедуры.

1. Определение и проверка нестандартного сетевого трафика.
2. Периодическая проверка привилегий и разрешений персонала для доступа к конкретным информационным ресурсам SCADA системы.
3. Отключение неиспользуемых протоколов, а также служб удаленного доступа и управления к сетевым узлам и приложениям.
4. Периодическое сканирование сетевых интерфейсов и драйверов.
5. Своевременное обновление ПО сетевых узлов из доверенных источников и т.д.

Известны три способа обнаружения атак в сетях.

1. Обнаружение по сигнатурам. Сигнатура определяет характеристики (профили) ранее совершенных атак. В процессе сканирования выявляется совпадение сигнатур и производится оповещение. Однако данный способ не позволяет выявить атаки с новыми (неизвестными) сигнатурами.

2. Обнаружение по аномальному поведению. Обнаружение атаки происходит при выявлении нештатного поведения сетевого узла/PLC или отклонений от нормального функционирования. Недостаток этого подхода в том, что на некорректную работу узла могут оказывать влияние и другие факторы, которые не имеют отношения к атакам, например, сбой оборудования или датчика и т.п.

3. Комбинированное обнаружение по спецификациям. Этот способ комбинирует два предыдущих, что позволяет компенсировать их недостатки.

Система обнаружения сетевых атак (Wireless Intrusion Detection System – WIDS) представляет программно-техническое решение, в состав которого входят программные агенты, выполняющие функцию сбора, обработки и анализа пакетов сетевого трафика. Агенты взаимодействуют с сервером, передают ему перехваченные пакеты. Сервер обрабатывает полученные данные на предмет обнаружения сигнатур атак и выявления аномального поведения сетевых узлов, а также реагирует на происходящие события. Таким образом, WIDS сочетает в себе сигнатурный и поведенческий способы и относится к третьему способу. В процессе работы система WIDS выполняет мониторинг и анализ трафика сенсорной сети. Ее функциональность включает следующие типовые процедуры.

1. Анализ топологии WSN.
2. Определение уязвимостей WSN.
3. Составление и ведение списков сетевых узлов. Такие списки формируются на основе анализа сетевого трафика и извлечения из перехваченных кадров MAC-адресов сетевых узлов. Полученные списки в дальнейшем фактически позволяют выявить появление в сети новых «чужих» потенциально опасных узлов.
4. Обнаружение и противодействие атакам в WSN. На данный момент число обнаруживаемых атак в WSN существенно отстает по количеству обнаруживаемых атак в проводных сетях, так как ограничивается лишь анализом трафика канального уровня модели OSI. Результатом обнаружения атаки является уведомление администратора о потенциальных проблемах различными способами (через электронную почту, SMS сообщения и т.п.) и запись в журнал событий – для последующего аудита.
5. Локализация источника атаки и ее подавление. WIDS могут использовать такие механизмы подавления, как: реализация DoS-атаки на узел злоумышленника, блокирование атакующего агента средствами активного сетевого оборудования. Локализация источника атак предусматривает определение координат устройства, нарушившего политику безопасности, по технологиям трилатерации, мультилатерации или триангуляции.
6. Контроль политики безопасности. Осуществляется на основе анализа списков сетевых узлов с целью обнаружения изменений в политиках, заданных администратором. В результате аудита можно обнаружить появление несанкционированных узлов и приложений, нарушения политики защиты трафика.
7. Проведение тестов на вторжение через существующие уязвимости SCADA системы и ее компонент специальными эксплоитами для пентестинга.
8. Мониторинг пропускной способности беспроводной сети и времени реакции сети. В процессе мониторинга система обнаружения атак может контролировать состояние физического и канального уровней сети и выявлять такие проблемы, как

a) перегрузка канала, узла или сети;
b) резкое увеличение числа кадров данных, поступающих на координатор, маршрутизаторы или оконечные узлы;
c) снижение уровня мощности радиосигналов;
d) резкое увеличение широковещательных служебных или маршрутных кадров;
e) перекрытие каналов связи с соседними сетями;
f) снижение пропускной способности сети без видимых причин;
g) резкое увеличение времени поиска маршрута;
h) резкое увеличение времени реакции серверных приложений на запросы клиентов;
i) увеличение коллизий в каналах передачи данных;
j) появление новых сетевых узлов;
k) снижение скорости передачи данных;
l) перегрузка сетевых узлов и сети в целом;
m) переполнение буферной памяти узлов, отказ обслуживания и т.п.

На основе анализа результатов такого контроля лицами, отвечающими за ИБ, принимаются необходимые решения и реализуются соответствующие меры оперативного и долгосрочного характера.

Заключение. Несмотря на достаточно большое количество возможных атак на беспроводные сенсорные сети и SCADA системы, наибольшую опасность представляют так называемые внутренние антропогенные угрозы ИБ. К ним следует отнести:

- неумышленные действия персонала, которые создают условия для проведения атак внешними злоумышленниками;
- сознательное неисполнение персоналом, обслуживающим SCADA системы, требований ИБ;
- недостаточная квалификация персонала в плане использования информационных технологий и реализации методов информационной защиты.

В отличие от внешнего злоумышленника, именно персонал предприятия может создавать большие возможности для проведения атак с целью заражения и распространения вредоносного кода по сенсорной сети. Проблемы ИБ часто вызваны не столько внешними атаками, сколько несоблюдением персоналом регламентов и правил ИБ предприятия или недостаточной квалификацией персонала в области информационных технологий. Диспетчеры и другой персонал предприятия могут пренебрегать своими обязанностями и в «свободное» время заниматься интернет-«серфингом», общением в социальных сетях, компьютерными играми. Результатом может быть несанкционированное заражение ПЭВМ компьютерными вирусами, троянами и червями, которые затем и проникают в сенсорные сети. Именно этим объясняется то, что вирусы и черви типа Stuxnet нередко присутствуют в промышленных системах, а факт их наличия обычно скрывается персоналом и руководителями, так как раскрытие данной информации приведет к проверке всего персонала и руководства с последующими выводами. Кроме того, обнаружение факта заражения SCADA системы может повлечь ее полную перезагрузку для очистки от вирусов и остановку технологического процесса, а это не всегда целесообразно с экономической точки зрения. Также недостаточная квалификация персонала, работающего с PLC и системой SCADA, требует привлечения сторонних специалистов для выявления и исправления изменений в ПО контроллеров, так как после очистки системы необходимо обеспечить, чтобы программы и установки параметров в контроллерах [9] соответствовали значениям, необходимым для нормальной работы всей системы промышленной автоматики.

Общеизвестно, что человеческий фактор является основным при отклонениях от нормального режима эксплуатации различных технических систем. Это требует особого внимания при создании и поддержании соответствующих технических регламентов.

Список литературы

1. Бершадский А. М. Классификация методов маршрутизации в беспроводных сенсорных сетях / А. М. Бершадский, Л. С. Курилов, А. Г. Финогеев // Известия 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 // Известия вузов. Поволжский регион. Технические науки. – Пенза : Изд-во ПГУ, 2012. – № 1. – С. 47–58.

3. 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.

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

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

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

7. Маслов В. А. Анализ, оценка и учет влияния помех радиопередающих устройств при построении беспроводных сетей с использованием технологии Wi-Fi в образовательных учреждениях / В. А. Маслов, А. Г. Финогеев // Надежность и качество : тр. междунар.симп. – 2009. – Т. 2. – С. 170–171.

8. Тюков А. П. Концепция супервизорного управления отоплением в коммерческих зданиях с использованием прогнозирующих моделей / А. П. Тюков, В. А. Камаев, М. В. Щербаков // Прикаспийский журнал: управление и высокие технологии. – 2012. – № 3 (19). – С. 71–76.

9. 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.

10. 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 // Известия вузов. Поволжский регион. Технические науки. – Пенза : Изд-во ПГУ, 2010. – № 3. – С. 27–36.

11. 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 // Известия ВолгГТУ. Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах». – 2011. – Т. 3, № 10. – С. 73–81.

12. 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. – Changsha, 2011. – P. 11–20.

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

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

15. 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.

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 Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh»* [News of Volgograd State Technical University. 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 Higher Educational Institutions. Volga region. Technical sciences]. Penza, Penza State University Publ., 2012, no. 1, pp. 47–58.

3. 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 analysis of models and methods of optimum choice of solutions for planning tasks in conditions of resource restrictions and risks]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2013, no. 3 (23), pp. 169–180.

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

5. Kamaev V. A., Natrov V. V. Analiz metodov otsenki kachestva funktsionirovaniya i effektivnosti sistem zashchity informatsii na predpriyatiyakh elektroenergetiki [Analysis of methods to assess the quality of functioning and effectiveness of information security systems for energy companies]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh»* [News of Volgograd State Technical University. Series "Actual problems of management, computer science and informatics in technical systems"], 2007, issue 1, no. 1, pp. 67–69.

6. Kamaev V. A., Natrov V. V. Metodologiya obnaruzheniya vtorzheniy [Intrusion Detection Methodology]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Kontseptualnoe proektirovanie v obrazovanii, tekhnike i tekhnologii»* [News of Volgograd State Technical University. Series "Conceptual design in education, engineering and technology"], 2006, issue 2, no. 2, pp. 127–132.

7. Maslov V. A., Finogeev A. G. Analiz, otsenka i uchet vliyaniya pomekh radioperedayushchikh ustroystv pri postroenii besprovodnykh setey s ispolzovaniem tekhnologii Wi-Fi v obrazovatelnykh uchrezhdeniyakh [Analysis, evaluation and account of the impact of interference of radio transmitting devices when building wireless networks using Wi-Fi technology in educational institutions]. *Nadezhnost i kachestvo: trudy mezhdunarodnogo simpoziuma* ["Reliability and quality": Proceedings of the International Symposium], 2009, vol. 2, pp. 170–171.

8. Tyukov A. P., Kamaev V. A., Shcherbakov M. V. Kontseptsiya supervizornogo upravleniya otopleniem v kommercheskikh zdaniyakh s ispolzovaniem prognoziruyushchikh modeley [Concept of supervisor heating control in commercial buildings using predictive models]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2012, no. 3 (19), pp. 71–76.

9. 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 heating network control based on wireless sensor networks]. *Prikladnaya informatika* [Applied Informatics], 2011, no. 3 (33), pp. 83–93.

10. 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 Higher Educational Institutions. Volga region. Technical sciences]. Penza, Penza State University Publ., 2010, no. 3, pp. 27–36.

11. Finogeev A. G., Maslov V. A., Finogeev A. A., Bogatyrev V. Ye. Monitoring i podderzhka prinyatiya resheniy v sisteme gorodskogo teplosnabzheniya na baze geterogennoy besprovodnoy seti [Monitoring and support of decision-making in the urban heat system based on heterogeneous wireless network]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh»* [News of Volgograd State Technical University. Series "Actual problems of management, computer science and informatics in technical systems"], 2011, vol. 3, no. 10, pp. 73–81.

12. 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. Changsha, 2011, pp. 11–20.

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

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

15. 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.