А. А. Финогеев, А. Г. Финогеев, И. С. Нефёдова, Е. А. Финогеев, В. А. Камаев, Анализ информационных рисков в системах обработки данных на основе «туманных» вычислений, *Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ.*, 2015, номер 4, 38–46

КОМПЬЮТЕРНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 681.518.3

А. А. Финогеев, А. Г. Финогеев,
И. С. Нефёдова, Е. А. Финогеев, В. А. Камаев

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ НА ОСНОВЕ «ТУМАННЫХ» ВЫЧИСЛЕНИЙ[1]

Рассматриваются аспекты управления информационными рисками в системах защищенного сбора и распределенной обработки больших сенсорных данных. Объектами информационных угроз являются компоненты SCADA-систем диспетчерского контроля и управления в службах энергоснабжения и энергопотребления. Сбор и распределенная обработка данных осуществляются пространственно распределенными датчиками, приборами автоматики, учета и контроля энергоносителей и процессов транспортировки энергии в инженерных энергетических сетях. На узлах беспроводной сенсорной сети, модемах сотовой связи и промышленных контроллерах приборов учета и контроля энергоресурсов реализуется модель распределенных «туманных» вычислений, относительно которой рассмотрены основные составляющие информационных рисков. Приведена классификация информационных угроз и атак в беспроводной транспортной среде «туманных» вычислений. Определены методы и инструментальные средства защиты сенсорных сетей, узлов сбора данных, беспроводных каналов связи и передаваемых данных. Особое внимание уделяется аспектам обеспечения информационной безопасности таких компонент системы «туманных» вычислений, как программные агенты и брокеры.

Ключевые слова: мониторинг, защита сенсорных данных, информационный риск, распределенная обработка данных, «туманные» вычисления, SCADA, беспроводная сенсорная сеть, информационная безопасность.

Введение

Понимание и оценка угроз информационной безопасности – это основа внедрения любой информационной системы, в том числе для обеспечения процессов мониторинга и диспетчерского контроля [1, 2]. Использование беспроводных каналов связи, особенно сетей сотовой связи, для передачи данных и реализации удаленного доступа многократно увеличивает риски информационной безопасности.

Традиционные системы управления рисками опираются на мнения экспертов либо предполагают ведение анкет, на основании которых производится оценка уязвимостей информационных систем и рисков. Это основной недостаток подобных систем, т. к. ответы могут давать некомпетентные лица либо лица, заинтересованные в сокрытии информации. Автоматизированные системы, основанные на базах знаний и процедурах логического вывода, позволяют выявлять информационные ресурсы, нарушение защиты которых является недопустимым; строить модели защиты информационных активов; сравнивать их между собой по критерию «эффективность – стоимость»; определять варианты комплексов мер защиты и контроля; вести мониторинг организации информационной безопасности. Вследствие того, что отечественные системы в настоящее время на рынке не представлены, недостатком является также высокая стоимость их покупки и использования.

Анализ рисков в системах сбора и обработки данных

Внедрение беспроводных сетей, технологий, моделей и методов сбора и распределенной обработки данных обусловливает возникновение новых опасностей, приводящих к убыткам или

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 15-37-50142, 15-07-01720, № 15-57-54033.

ущербу в результате их применения в системах мониторинга. Анализ информационных рисков представляется как процесс выявления подобных опасностей и оценки негативных последствий в результате возникновения нарушений в работе вычислительных, программных и телекоммуникационных составляющих и технологических процессов сбора, обработки, хранения и передачи информации, а также как прогнозирование последствий в количественных показателях. Потенциально возможные негативные последствия могут возникнуть в результате сбоев или отказов в работе распределенных на большой территории сенсорных узлов, модемов, измерительного, технологического оборудования, телекоммуникационных систем передачи данных. Причиной возникновения и реализации рисков могут быть деструктивные воздействия вирусных программ, ошибки или преднамеренные действия персонала предприятия и внешних злоумышленников, факторы окружающей среды, сбои электропитания, помехи и т. п.

Новой технологией распределенной обработки больших сенсорных данных, которая предлагается для систем мониторинга и диспетчерского управления, является модель «туманных» вычислений [3, 4]. Концепция «туманных» вычислений предусматривает обработку данных терминальными устройствами с ограниченными вычислительными и энергетическими ресурсами, в число которых могут входить контроллеры промышленного оборудования и устройств бытовой техники, а также узлы сенсорных сетей. В качестве защищаемых компонент системы «туманных» вычислений необходимо рассматривать операционные прошивки, программные агенты и брокеры, которые реализуют процедуры сбора и обработки данных, а также сами данные, передаваемые по каналам связи.

Понятие информационного риска включает в себя следующие категории: активы предприятия, причины или угрозы, факторы, уязвимости, последствия, ущерб [5]. Причина или угроза возникновения информационного риска (рис. 1) – это явление или событие, вызывающее риск, а фактор риска определяется как характеристика процесса или явления, которое способствует или препятствует возможности реализации риска [6].

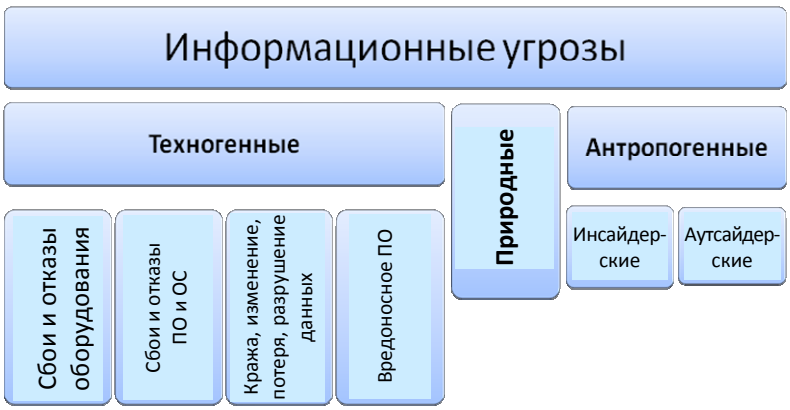

Рис. 1. Виды информационных угроз

Информационная угроза определяется источниками информационных рисков и реализуется через уязвимости системы мониторинга, причем факторы могут способствовать или препятствовать реализации рисков. Большинство угроз реализуется путем осуществления атак на информационные активы внутренними и внешними нарушителями и (или) программными средствами с использованием уязвимостей (рис. 2).

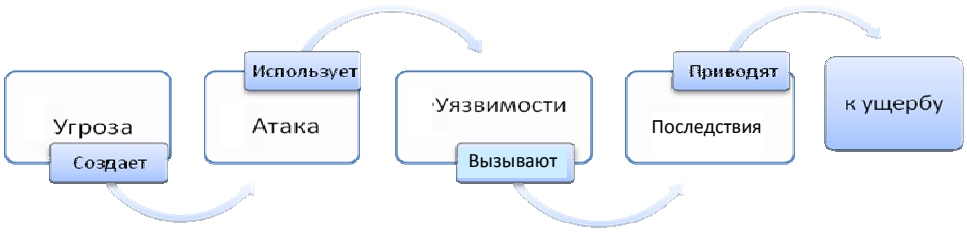

Рис. 2. Взаимосвязь между видами информационного риска

Управление информационными рисками заключается в согласованном воздействии на объекты и субъекты информационно-вычислительной и телекоммуникационной инфраструктуры системы энергетического мониторинга в направлении устранения угроз, уязвимостей и факторов рисков с целью предупреждения или минимизации возможных последствий от их реализации.

Модель информационных рисков может быть представлена в виде взвешенного динамического гиперграфа (рис. 3): $G = (V(S_i, Q_j), P_k(U_k))$, где подмножество вершин $S_i = \{s_i | i = 1, ..., N_s\}$ моделирует угрозы, подмножество вершин $Q_j = \{q_j | j = 1, ..., N_q\}$ – уязвимости, множество гиперребер $P_k = \{p_k | k = 1, ..., M\}$ – атаки, динамически возникающие в момент времени t.

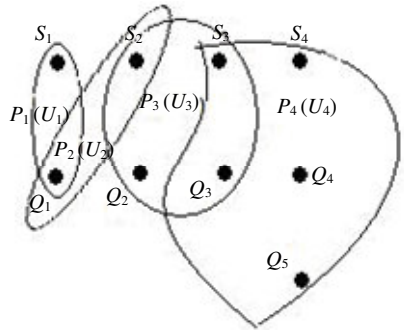

Рис. 3. Гиперграфовая модель информационных рисков

Динамические гиперребра объединяют подмножество вершин-угроз с подмножеством вершин-уязвимостей и представляют собой атаки, в результате которых возникает и реализуется информационный риск R_k, вызывающий последствия, которые можно оценить величиной ущерба U_k. В модели величина возможного ущерба U_k, d, случае реализации информационного риска, представлена весом динамического гиперребра. Оценка информационного риска представляет собой определение уровня риска, а также его сравнение с допустимым уровнем при конкретных условиях его реализации. Для оценки риска можно использовать такие параметры, как уровень критичности K_i возникновения i-й угрозы, %, и вероятность реализации атаки P_a со стороны угрозы S_i, %, через уязвимость системы Q_j.

Уровень критичности информационного риска можно оценить как отношение числа реализаций риска к числу возникновений риска в течение интервала времени ΔT:

$$K_r = \frac{N_{\text{реал}}}{N_{\text{воз}}} \Delta T.$$

Угрозу можно оценить как $S_i (Qj) = K_i \cdot P_a \cdot 0{,}1$, где коэффициент 0,1 используется для снижения размерности при перемножении переменных в процентах.

Информационный риск R можно оценить как $R_i = P_i(VF)\, U_i = (P_i(V)\, P_i(F/V))\, U_i$, где $P_i(VF)$ – вероятность совместного возникновения риска для i-й угрозы (событие V) и его реализации (событие F); $P_i(V)$ – вероятность возникновения риска из-за i-й угрозы; $P_i(F/V)$ – условная вероятность реализации риска (события F) при наступлении события V; U_i – уровень ущерба от реализации риска (события F).

Вероятность реализации информационного риска определим с учетом уязвимости $P_i(V) = P_j^u \cdot Q_i$, где P_i^u – вероятность реализации i-й угрозы в отношении j-го актива; Q_i – величина i-й уязвимости.

Величину риска R определим как $R = \sum_{i=1}^{n} (P_i^u \cdot P_i(F/V) Q_i \cdot U_i)$.

Управление информационными рисками в автоматизированных системах мониторинга и диспетчерского управления должно быть организовано в соответствии с политикой информационной безопасности предприятия [7, 8]. Здесь используются документально задекларированные правила, процедуры и разрешения, которые доводятся администраторами информационной безопасности и руководством до персонала для исполнения и являются инструментами управления рисками.

Обеспечение информационной безопасности в SCADA-системах с распределенной обработкой данных

Защита от угроз безопасности является важным элементом в процессе функционирования SCADA-систем. Для обеспечения информационной безопасности SCADA-систем, которые обслуживают пространственно распределенные объекты инженерных энергетических сетей, необходима защита таких компонент, как:

1. Контроллеры приборов автоматики, учета и контроля.
2. Сенсорные узлы и модемное оборудование сотовой связи.
3. Узлы серверного кластера в центре обработки данных.
4. Информационное хранилище.
5. Гетерогенная беспроводная среда передачи данных.

Эффективность решения задач по обеспечению информационной безопасности зависит от технологий и средств защиты беспроводной транспортной среды передачи данных. При реализации модели «туманных» вычислений, когда операции по распределенной обработке данных выполняются на терминальных и ретранслирующих узлах сенсорной сети и в промышленных контроллерах, также требуется организация защиты программных агентов и брокеров, загружаемых в данные узлы. В целом вопросы, касающиеся обеспечения информационной безопасности, смещаются от защиты периметра сети в сторону защиты передаваемых данных и самих приложений «туманных» вычислений.

Программные агенты, брокеры и серверные приложения SCADA-системы должны иметь доступ только к внутренним ресурсам (сенсорные данные и данные из центрального информационного хранилища). «Тонкие» пользовательские клиентские приложения в виде информационных панелей (дашбордов) на мобильных средствах связи и вычислительных узлах за пределами периметра могут иметь ограниченный доступ только к агрегатам сенсорных данных и интегральным показателям, если это разрешено политикой безопасности. Хотя такая защита периметра не гарантирует полную безопасность всех распределенных ресурсов в модели «туманных» вычислений, ее существование дает администраторам возможность осуществлять контроль доступа к информационным активам и оперативно обнаруживать вторжения. Для защиты периметра необходимо установить на координаторах сенсорных сегментов модули проверки адресов источников и обнаружения внешнего трафика, за исключением запросов на сбор данных и маршрутных кадров от центрального координатора, а также запросов от тех пользовательских устройств, адреса которых загружаются в память координаторов сегментов. Необходимо обеспечить криптографическую защиту передаваемых данных и контроль передачи данных по беспроводным каналам связи между брокерами «туманных» вычислений и центральным координатором сети, а также между клиентами и шлюзами.

Ограниченные энергоресурсы и вычислительная мощность узлов сенсорных сетей не позволяют применять сложные протоколы и алгоритмы защиты данных и процессов передачи. Основное внимание уделяется своевременному обнаружению подозрительного трафика либо несвойственных маршрутов передачи данных, поэтому инструментами информационной безопасности в беспроводных сенсорных сетях следует считать системы обнаружения (IDS – Intrusion Detection System) и предотвращения вторжений (IPS – Intrusion Prevention System) [9].

Критической угрозой для систем диспетчерского контроля и управления технологическими процессами является внедрение программ для кражи данных о контролируемых процессах или кодов активации исполнительных механизмов. Серьезной проблемой для SCADA-систем, которые работают с множеством удаленных объектов мониторинга на большой территории, является тенденция к установке модемов сотовой связи для сбора данных и использованию в качестве передающей среды каналов сотовой связи с возможностью публичного доступа. Такие каналы являются фактически мишенью для проведения атак на информационные активы.

В беспроводной сенсорной сети SCADA-систем нового поколения могут быть реализованы следующие виды атак (рис. 4) [10].

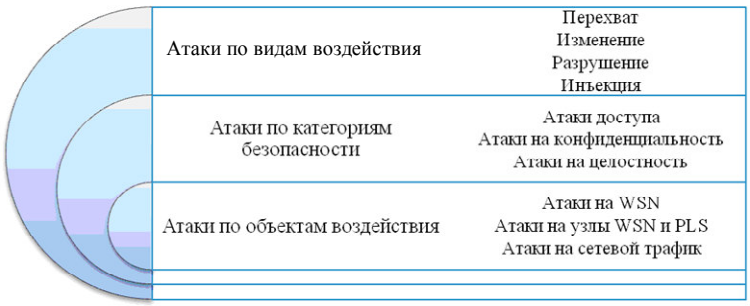

Рис. 4. Виды информационных атак в беспроводной сенсорной сети (WSN)

Все атаки можно классифицировать по отношению ко всей сети, отдельным узлам и сетевому трафику (рис. 5) [11].

Рис. 5. Классификация атак

В процессе создания механизмов защиты от подобных атак необходимо учитывать следующие моменты:

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».

2. При работе алгоритмов маршрутизации используется механизм широковещательной рассылки маршрутных кадров и квитанций подтверждения. Широковещательная рассылка используется также при конфигурировании сети, назначении адресов 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.

5. Идентификация сенсорных узлов и кадров данных осуществляется только на основе адресной информации, полученной сенсорными узлами от координатора сети, что позволяет подменить координатор.

6. Аутентификация кадров данных и узлов сети в большинстве случаев не выполняется, что позволяет подменить сенсорные узлы и маршрутизаторы «чужими» узлами с вредоносной «прошивкой».

Инструменты обеспечения безопасности в среде «туманных» вычислений

Для обеспечения надежной и безопасной передачи данных беспроводная транспортная среда SCADA-системы должна быть устойчивой как к радиопомехам, так и к различным видам воздействий, приводящих к нарушению ее функциональности, сбоям и отказам в работе сетевых узлов и подключенных к ним устройств. Обеспечение помехоустойчивости требует реализации мероприятий по электромагнитной защите узлов сети (экранирование узлов, использование узконаправленных антенн, применение фильтров помех, помехоустойчивое кодирование данных, расширение спектра частот, активная смена радиоканалов), что позволяет устранить или снизить влияние помех.

Для решения проблем безопасности целесообразно использовать следующие методы.

1. Резервирование транспортной среды путем создания вторичной сети, которая активируется при обнаружении атаки на основную сеть.

2. Интеграция в систему мониторинга программно-технических решений по обнаружению и предотвращению вторжений, которые могут поставляться разработчиками или представлять собой автономные комплексы.

3. Использование встроенных подсистем обеспечения безопасности.

4. Комбинированные решения.

Основными мероприятиями защиты являются:

– планирование беспроводной сенсорной сети и конфигурирование сенсорных узлов;

– идентификация и аутентификация всех активов системы мониторинга (пользователи, программные агенты и брокеры, серверные и клиентские приложения, сетевые узлы, приборы автоматики, кадры данных);

– организация защиты от активных радиопомех;

– шифрование и организация защищенных каналов передачи данных;

– контроль и управление ключами доступа и шифрования;

– поиск и ликвидация уязвимостей в проприетарном программном обеспечении системы;

– локализация атак и злоумышленников;

– обнаружение и предотвращение вторжений;

– контроль трафика в реальном времени и фильтрация кадров данных;

– анализ и ликвидация последствий атак целью восстановления функциональности системы после сбоев и отказов;

– мониторинг и аудит системы безопасности;

– отслеживание и установка обновлений ПО и ОС в ручном режиме;

– отслеживание информации в сети Интернет по уязвимостям эксплуатируемой SCADA-системы у других потребителей и производителя;

– периодическое использование эксплоитов с новыми базами уязвимостей для пентестинга эксплуатируемых компонент системы мониторинга;

– аудит работы агентов, приложений и пользователей и т. д.

К основным средствам обеспечения безопасности следует отнести:

1. Системы обнаружения сетевых вторжений (NIDS – Network-Based Intrusion Detection System).

2. Системы предотвращения вторжений через периметр сети (NIPS – Network-Based Intrusion Prevention System).

3. Автономные системы предотвращения вторжений, размещаемые на сетевых узлах (HIPS – Host-Based Intrusion Prevention System).

4. Системы антивирусной защиты.

5. Межсетевые экраны.

6. Системы аутентификации и управления доступом пользователей.

7. Системы аутентификации сетевых ресурсов и кадров данных.

8. Системы криптографической защиты и управления ключами и т. п.

Заключение

От степени защищённости систем мониторинга и диспетчерских SCADA-систем в области энергетики зависят энергетическая безопасность регионов и национальная безопасность. Методы управления информационными рисками на базе инфокоммуникационных технологий яв-

ляются достаточно новым направлением в теории управления рисками. Они касаются разработки мероприятий по снижению вероятности возникновения и реализации информационных рисков в плане предупреждения несанкционированного доступа к данным, возможности перехвата, изменения, уничтожения данных и в конечном счете предотвращения аварий и сбоев оборудования на объектах инженерных коммуникаций энергетической отрасли. В общей инфраструктуре системы мониторинга с использованием распределенной обработки данных на основе модели «туманных» вычислений следует выделять три зоны ответственности с точки зрения реализации мероприятий безопасности.

1. Зону транспортной среды для сбора, распределенной обработки и передачи данных на основе беспроводной сенсорной сети и каналов сотовой связи, в которой узлы сенсорной сети и модемы сотовой связи связаны с датчиками, контроллерами и исполнительными механизмами.

2. Зону пользовательского интерфейса, в которой работают операторы и диспетчеры SCADA-систем и ведут наблюдения за объектами мониторинга и ходом контролируемого технологического процесса.

3. Зону доступа к распределенному информационному хранилищу со стороны серверных приложений вычислительного кластера и со стороны клиентских приложений пользовательских вычислительных устройств и средств мобильной связи.

Для защиты информационных активов предприятий энергетики целесообразно использовать многослойную модель, включающую защиту персональных данных и учетных записей персонала, списки контроля доступа, механизмы контроля периметра транспортной среды и отдельных сетевых сегментов, виртуальные защищенные каналы связи, защиту центрального вычислительного кластера и т. д. Однако обеспечение защиты и выполнение правил политики безопасности при организации доступа с подобных устройств к агентам и брокерам «туманных» вычислений требуют разработки новых моделей защиты из-за ограниченных вычислительных и энергетических ресурсов сетевых узлов. При этом вопросы информационной защиты смещаются от защиты периметра сети и сетевой инфраструктуры в сторону защиты сенсорных данных и программных агентов, распределенных по узлам беспроводной среды «туманных» вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. *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.

2. *Kamaev V. A.* Wireless monitoring and control at urban heating supply system / V. A. Kamaev, L. R. Fionova, A. G. Finogeev, A. A. Finogeev // International Journal of Applied Engineering Research – Research India Publications. 2015. Vol. 10, no. 3. P. 6499–6507.

3. *Bonomi F.* Fog Computing and its Role in the Internet of Things / F. Bonomi, R. Milito, J. Zhu, S. Addepalli // Proceedings of the first edition of the MCC workshop on Mobile cloud computing. 2012. P. 13–16.

4. *Камаев В. А.* Инструментальные средства «облачного» мониторинга распределенных инженерных сетей / В. А. Камаев, А. Г. Финогеев, И. С. Нефедова, Е. А. Финогеев // Изв. Волгоград. гос. техн. ун-та. Сер.: Актуальные проблемы управления, вычислительной техники и информатики в технических системах. 2014. № 25 (152). Вып. 20. С. 164–176.

5. *ISO/IEC* 27005:2008. Information technology. Security techniques. Information security risk management // URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en.

6. *Финогеев А. Г.* Проблемы безопасности беспроводной сенсорной сети в SCADA-системах АСУ ТП / А. Г. Финогеев, И. С. Нефедова, Тхай Куанг Винь // Изв. Волгоград. гос. техн. ун-та. Сер.: Актуальные проблемы управления, вычислительной техники и информатики в технических системах. 2014. № 6 (133). Вып. 20. С. 129–138.

7. *Завгородний В. И.* Информационные риски и экономическая безопасность предприятия / В. И. Завгородний. М.: Финакадемия, 2008. 160 с.

8. *ГОСТ Р 50922-2006*. Защита информации. Основные термины и определения // URL: http://www.altell.ru/legislation/standards/50922-2006.pdf.

9. *Камаев В. А.* Методология обнаружения вторжений / В. А. Камаев, В. В. Натров // Изв. Волгоград. гос. техн. ун-та. Сер.: Концептуальное проектирование в образовании, технике и технологии. 2006. Вып. 2, № 2. С. 127–132.

10. *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.

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

Статья поступила в редакцию 31.08.2015

ИНФОРМАЦИЯ ОБ АВТОРАХ

Финогеев Антон Алексеевич – Россия, 440026, Пенза; Пензенский государственный университет; канд. техн. наук, доцент кафедры «Системы автоматизированного проектирования»; antonfinogeev@mail.ru.

Финогеев Алексей Германович – Россия, 440026, Пенза; Пензенский государственный университет; д-р техн, наук, профессор; профессор кафедры «Системы автоматизированного проектирования»; alexeyfinogeev@gmail.com.

Нефёдова Ирина Сергеевна – Россия, 440026, Пенза; Пензенский государственный университет; аспирант кафедры «Системы автоматизированного проектирования»; nefedya2008@yandex.ru.

Финогеев Егор Алексеевич – Россия, 440026, Пенза; Пензенский государственный университет; аспирант кафедры «Системы автоматизированного проектирования»; frzegor@yandex.ru.

Камаев Валерий Анатольевич – Россия, 400131, Волгоград; Волгоградский государственный технический университет; д-р техн, наук, профессор; зав. кафедрой «Системы автоматизированного проектирования и поискового конструирования»; Vkamaev40@mail.ru.

A. A. Finogeev, A. G. Finogeev,
I. S. Nefedova, E. A. Finogeev, V. A. Kamaev

ANALYSIS OF INFORMATION RISKS IN THE SYSTEM OF DISTRIBUTED MONITORING BASED ON THE FOG COMPUTING MODEL

Abstract. The paper considers the aspects of information risk management in the systems of secured collection and distributed processing of huge sensor data. The objects of information threats are components of SCADA-systems of dispatch control and management in the services in energy supply and consumption. Collection and distribution of data processing are carried out spatially with the distributed sensors, devices of automation, accounting and control of energy sources and energy transport processes in the engineering of energy networks. At the wireless sensor network nodes, cellular modems and industrial controllers, metering and control of energy, a model of distributed "fog" calculations, with respect to which the basic components of information risks are considered, is actualized. The classification of information threats and attacks in the wireless transport medium "fog" calculations is presented. The methods and tools of protection of wireless sensor network (WSN), data collection nodes, wireless communications and data transmission are determined. Particular attention is paid to information security aspects of such a component of the "fog" computing as software agents and brokers.

Key words: monitoring, sensor data protection, information risk, distributed data processing, "fog" computing, SCADA, wireless sensor network, information security.

REFERENCES

1. Finogeev A. G., Dil'man V. B., Maslov V. A., Finogeev A. A. Sistema udalennogo monitoringa i upravleniia setiami teplosnabzheniia na osnove besprovodnykh sensornykh setei [System of remote monitoring and control of heat supply networks based on the sensor networks]. *Prikladnaia informatika*, 2011, no. 3 (33), pp. 83–93.

2. Kamaev V. A., Fionova L. R., Finogeev A. G., Finogeev A. A. Wireless monitoring and control at urban heating supply system. *International Journal of Applied Engineering Research – Research India Publications*, 2015, vol. 10, no. 3, pp. 6499–6507.

3. Bonomi F., Milito R., Zhu J., Addepalli S. Fog Computing and Its Role in the Internet of Things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012. P. 13–16.

4. Kamaev V. A., Finogeev A. G., Nefedova I. S., Finogeev E. A. Instrumental'nye sredstva «oblachnogo» monitoringa raspredelennykh inzhenernykh setei [Tools of "fog" monitoring of distributed engineering networks]. *Izvestiia Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Aktual'nye problemy upravleniia, vychislitel'noi tekhniki i informatiki v tekhnicheskikh sistemakh*, 2014, no. 25 (152), iss. 20, pp. 164–176.

5. *ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management*. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en.

6. Finogeev A. G., Nefedova I. S., Tkhai Kuang Vin'. Problemy bezopasnosti besprovodnoi sensornoi seti v SCADA-sistemakh ASU TP [Issues of safety of wireless sensor network in SCADA-systems of ACS TP]. *Izvestiia Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Aktual'nye problemy upravleniia, vychislitel'noi tekhniki i informatiki v tekhnicheskikh sistemakh*, 2014, no. 6 (133), iss. 20, pp. 129–138.

7. Zavgorodnii V. I. *Informatsionnye riski i ekonomicheskaia bezopasnost' predpriiatiia* [Information risks and economic safety of an enterprise]. Moscow, Finakademiia Publ., 2008. 160 p.

8. *GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniia* [Data protection. Basic terms and definitions]. Available at: http://www.altell.ru/legislation/standards/50922-2006.pdf.

9. Kamaev V. A., Natrov V. V. Metodologiia obnaruzheniia vtorzhenii [Methods of invasion determination]. *Izvestiia Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Kontseptual'noe proektirovanie v obrazovanii, tekhnike i tekhnologii*, 2006, iss. 2, no. 2, pp. 127–132.

10. 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, vol. 11 (11s), pp. 384–388.

11. Finogeev A. G., Nefedova I. S., Finogeev E. A., Tkhai Kuang Vin', Botvinkin P. V. Analiz i klassifikatsiia atak cherez besprovodnye sensornye seti v SCADA-sistemakh [Analysis and classification of threats through wireless networks in SCADA-systems]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii*. Astrakhan, 2014, no. 1, pp. 12–23.

The article submitted to the editors 31.08.2015

INFORMATION ABOUT THE AUTHORS

Finogeev Anton Alekseevich – Russia, 440026, Penza; Penza State University; Candidate of Technical Sciences, Assistant Professor of the Department "Systems of Automated Design"; antonfinogeev@mail.ru.

Finogeev Alexey Germanovich – Russia, 440026, Penza; Penza State University; Doctor of Technical Sciences, Professor; Professor of the Department "Systems of Automated Design"; alexeyfinogeev@gmail.com.

Nefedova Irina Sergeevna – Russia, 440026, Penza; Penza State University; Postgraduate Student of the Department "Systems of Automated Design"; nefedya2008@yandex.ru.

Finogeev Egor Alekseevich – Russia, 440026, Penza; Penza State University; Postgraduate Student of the Department "Systems of Automated Design"; frzegor@yandex.ru.

Kamaev Valery Anatolevich – Russia, 440026, Volgograd; Volgograd State Technical University; Doctor of Technical Sciences, Professor; Head of the Department "Systems of Automated Design"; Vkamaev40@mail.ru.