УДК 007.956

ОНТОЛОГИЯ КАК ОСНОВА ДЛЯ РАЗРАБОТКИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Т.Н. Ворожцова

Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, Иркутск, Россия

tnn@isem.sei.irk.ru, tnvr@yandex.ru

Аннотация

В статье описывается онтология кибербезопасности, разработанная на базе стандартов. В качестве основы был использован международный стандарт ISO/IEC 27032:2012 «Руководящие указания по кибербезопасности», разработанный подкомитетом № 27 (SC 27) по информационной безопасности первого объединенного технического комитета (JTC 1) ISO и IEC. Рассматриваются основные понятия, связанные с проблемой обеспечения кибербезопасности и их взаимосвязи. Исследуется возможность проектирования базовой структуры интеллектуальной системы обеспечения кибербезопасности объектов энергетики на основе формализованного представления этих понятий и связей.

Ключевые слова: *кибербезопасность, онтология, информационная безопасность, интеллектуальная система, формализация знаний.*

Введение

В Институте систем энергетики им. Л.А. Мелентьева Сибирского отделения РАН (ИСЭМ СО РАН) в связи с разработкой новой технологической платформы ЕЭС России – интеллектуальной энергосистемы с активно-адаптивной сетью (ИЭС ААС) все большее внимание уделяется вопросам обеспечения кибербезопасности энергетических объектов и систем, которые относятся к наиболее важным объектам критической инфраструктуры [1, 2].

В связи с неограниченным ростом количества разнообразных компьютерных устройств, использующихся в управлении сложными техническими системами, все острее проявляется проблема не только защиты данных и информации, но и обеспечения безопасности людей и объектов, таких как объекты энергетики, энергетические магистральные сети и т.п. Появились такие понятия как кибератаки, кибертерроризм, кибервойна.

В статье рассматривается попытка разработки онтологии, описывающей основные понятия и их взаимосвязи, имеющие отношение к проблеме кибербезопасности в системах энергетики.

1 Онтология как средство формализации знаний при разработке интеллектуальных систем

Обеспечение кибербезопасности объектов энергетики предполагает совокупность технологий, процессов, методов защиты компьютерного оборудования, информации, программ, услуг, сетей от непреднамеренного или несанкционированного доступа, изменения и разрушения, в том числе от незапланированных событий и стихийных бедствий. Решение такой сложной задачи невозможно без использования современных средств интеллектуализации информационных технологий, которые должны не просто обеспечить

быструю обработку большого количества данных, но и выполнять оценку состояния окружающей среды, в которой работает техническая система.

Проектируемая интеллектуальная система (ИС) обеспечения кибербезопасности (ИСОК) должна решать такие задачи, как накопление и анализ поступающих данных; мониторинг данных – их интерпретация в реальном масштабе времени; диагностика работы компьютерных систем управления и выявление отклонений от нормального режима работы; прогнозирование последствий некоторых событий; поддержка принятия решений в виде своевременного предоставления необходимой информации и рекомендаций.

Онтология является средством, обеспечивающим концептуальный уровень представления знаний, необходимых при разработке данной ИС. В частности использование онтологии дает возможность сформировать структуру ИС, описать набор компонентов и их взаимосвязей, сформировать список решаемых задач с привязкой к данным и программным компонентам, а также обеспечить гибкий интерфейс с учетом потребностей конкретного пользователя.

2 Терминология по кибербезопасности

Основная терминология, связанная с проблемой кибербезопасности, описана в стандарте ISO/IEC 27032:2012, разработанном подкомитетом № 27 (SC 27) по информационной безопасности первого объединенного технического комитета (JTC 1) ISO и IEC – «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» [3, 4]. Данный стандарт предназначен для объединения усилий разных заинтересованных сторон, взаимодействующих в среде Интернет. Обязательным для применения вместе с указанным стандартом является стандарт ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

Стандарт по кибербезопасности рассматривает понятие кибербезопасности с точки зрения его отличий по отношению к безопасности информационных систем и сетей, информационной безопасности и безопасности Интернет. В связи с этим, дополнительно используются термины и определения, описанные в ГОСТ Р 53114-2008 «Обеспечение информационной безопасности в организации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [5, 6].

Кибербезопасность означает обеспечение конфиденциальности, целостности и доступности информации в киберпространстве, а также ее подлинности, наблюдаемости, достоверности. В соответствии с указанным стандартом, кибербезопасность опирается на информационную безопасность, безопасность приложений, сетевую безопасность и безопасность Интернет.

«**Киберпространство** представляет собой некую сложную сущность, которая существует объективно и проявляется во взаимодействии людей, программного обеспечения и сервисов Интернет. Существование киберпространства поддерживается физическими сетями связи, распределенными по всему миру, оборудованием и информационно-коммуникационными технологиями» [7].

Кроме определения этих понятий, стандарт по кибербезопасности отражает взаимосвязи между следующими основными понятиями:

- **Стейкхолдеры** – причастная или заинтересованная сторона, персона или организация, которая может воздействовать на деятельность или принятие решений. Согласно стандарту все стейкхолдеры в киберпространстве делятся на потребителей,

пользующихся услугами, доступными в киберпространстве, и провайдеров, обеспечивающих доступ в киберпространство или являющихся поставщиками услуг виртуального мира. Стейкхолдерами в энергетике являются собственники предприятий, инвесторы, партнеры и конкуренты, общественные организации и органы власти, а также клиенты и сотрудники предприятий. На стейкхолдерах лежит основная ответственность за обеспечение безопасности активов, для которых они представляют ценность.

- **Активы** в киберпространстве как ресурсы, ценные для личности, организации или государства могут быть материальными и нематериальными. К материальным активам относятся имущество предприятия, здания, оборудование, машины, запасы сырья. Нематериальными активами являются доступ к услугам или предоставление услуг, владение патентами или важной информацией, квалификация, опыт, репутация сотрудников. Кроме этого, существуют виртуальные активы, например, виртуальная валюта. Обеспечение кибербезопасности означает защиту активов от киберугроз.
- **Угрозы** в стандарте по кибербезопасности означают потенциально нежелательные воздействия, в результате которых может быть причинен вред системе, личности или организации. Угрозы рассматриваются в их привязке к активам и делятся на:
    - угрозы персональным активам (раскрытие персональных данных, несанкционированное использование оборудования пользователя, угроза виртуальным активам);
    - угрозы активам организации (искажение финансовых данных, доступ к секретной информации, негативное информационное воздействие через сайт организации).
- **Нарушители и агенты угроз** – это отдельные индивидуумы либо их группы, которые играют определенные роли в осуществлении нападения или в его поддерживании.. Угрозы кибербезопасности, как правило, ассоциируются с определенными активами. Решающее значение в оценивании рисков и создании соответствующих систем реагирования имеет понимание намерений (развлечения или шпионаж) и мотивов нарушителей и агентов угроз, которые могут быть, например, политическими или экономическими, а также их возможностей – осведомленности, степени доступа, размеров финансирования и т.п.
- **Риски.** Одним из распространенных понятий, связанных с кибербезопасностью, является "риск", как наиболее распространенная оценка степени опасности, вероятности причинения вреда или потерь того или иного вида. С другой стороны, понятие риска обусловлено наличием неопределенности результата деятельности как субъекта, так и объекта кибербезопасности. Риски кибербезопасности представляют некий сложный комплекс, который зависит еще и от типов взаимосвязей: «бизнес-бизнес», «предприятие–потребитель» или «потребитель–потребитель».
- **Уязвимость** – это слабое звено в составе актива или системы управления, через которое может быть реализована угроза. В соответствии с ГОСТ Р 53114-2008 уязвимость определяется как внутреннее свойство объекта, создающее восприимчивость к воздействию источника риска, которое может привести к какому-либо последствию. Наличие уязвимостей позволяет внедряться в коды приложений и выполнять непредусмотренные или несанкционированные действия, нарушая их работу, целостность систем или данных. В системах управления техническими объектами важно знать, в первую очередь, уязвимости информационных систем.
- **Меры кибербезопасности**. Стандарт ISO/IEC 27032:2012 рассматривает следующие ключевые меры кибербезопасности:
    - на уровне защиты приложений меры кибербезопасности включают в себя, например, использование безопасных механизмов повышения эффективности

сессий в веб-приложениях, проверку правильности вводимых и получаемых данных для предотвращения атак, использование безопасных сценариев, предотвращающих возможность распространения атак, проверку подлинности свидетельств сервиса и др.

- на уровне защиты серверов от несанкционированного доступа стандарт предлагает такие меры, как:
  - конфигурирование серверов и операционных систем с возможностью обеспечения аудита событий безопасности и других системных нарушений;
  - внедрение системы мониторинга и развертывания обновлений безопасности и обновлений безопасности;
  - использование на серверах антивирусных программ;
  - регулярное тестирование всего существующего и загруженного контента антивирусными сервисами;
  - регулярное тестирование уязвимости сайтов и приложений для оценки степени адекватности используемых механизмов безопасности;
  - проявление активного внимания к любым рискам, угрозам, опасностям и отклонениям в нормальном функционировании систем.
- на уровне защиты конечных пользователей меры кибербезопасности включают:
  - использование операционных систем и новейших версий прикладного программного обеспечения с установленными обновлениями системы безопасности;
  - использование антивирусных сервисов;
  - включение блокираторов для контроля выполнения на локальном компьютере скриптов, полученных исключительно из источников, заслуживающих доверия;
  - использование фишинг-фильтров;
  - использование брандмауэров и систем обнаружения вторжений (IDS);
  - использование автоматического обновления, гарантирующего системную установку новейших пакетов безопасности.
- в отношении атак социального инжиниринга основными аспектами кибербезопасности являются организационно-распорядительные, включающие, например, разработку основных правил работы с информацией и формирование политики безопасности; функционально-когнитивные, такие как категорирование информации, подготовка и тестирование сотрудников; технологические меры – использование механизмов аутентификации пользователей и сертификации используемых сервисов.

3 Некоторые аспекты кибербезопасности объектов энергетики

Для формирования онтологии кибербезопасности используем некоторые методологические аспекты исследования проблемы безопасности, рассмотренные в работах Атаманова Г.А. [8, 9].

По отношению к таким сложным техническим системам, как объекты энергетики, понятия «киберопасность»/«кибербезопасность» рассматриваются как некоторое сочетание условий, определенная «ситуация», характеризующая положение и взаимодействие этого объекта с окружающей средой, которое субъект считает соответственно опасной или безопасной. Окружающей средой в данном случае является киберпространство, а субъектом

– управляющая данным техническим объектом структура того или иного уровня, от персонального до государственного.

Понятие «безопасность», в том числе и «кибербезопасность» имеет непосредственное отношение к объекту безопасности. Объект энергетики является очень сложной системой и его кибербезопасность может быть обеспечена при условии, что обеспечена безопасность всех его элементов, которые имеют контакты с киберпространством. Поэтому выявление таких структурных элементов при проектировании системы обеспечения кибербезопасности является необходимым исходным условием.

В соответствии с рассматриваемым в данной работе стандартом, объектами защиты являются так называемые активы, материальные и нематериальные. Обеспечение кибербезопасности зависит от их видов. Вторым важным этапом является изучение активов, требующих защиты, их классификация, ранжирование, выявление уязвимостей и возможных угроз.

Заинтересованные в защите этих активов участники или стэйкхолдеры являются субъектами кибербезопасности, которые, с одной стороны, должны оценивать и обеспечивать кибербезопасность активов, но, с другой стороны, могут рассматриваться как объекты кибербезопасности, а в некоторых случаях могут быть и источниками угроз или нарушителями.

При рассмотрении понятия «кибербезопасность» необходимо исследовать возможные киберопасности или угрозы. Как уже было отмечено, по стандарту угрозы рассматриваются в их привязке к активам. В современных условиях информационных и кибервойн количество угроз и их разновидностей постоянно растет. Киберопасности или киберугрозы при современном уровне компьютеризации технических объектов существуют всегда, хотя они могут и не проявляться до некоторого момента. Даже при самых надежных средствах защиты кибербезопасность может быть только относительной, гарантированной с некоторой вероятностью. Поэтому необходимой компонентой ИС киберзащиты должна быть система мониторинга, накапливающая знания не только о выявленных и предотвращенных угрозах, но и потенциальных.

При оценке ситуации, характеризующей степень киберопасности или кибербезопасности объекта энергетики, необходимо учитывать некоторую совокупность факторов, текущую ситуацию, описывающую взаимодействие объекта с элементами киберпространства, для этого выполнить анализ:

- объекта, его структурных элементов и их ранжирование с точки зрения уязвимости и способности сохранять основные свойства и характеристики для выполнения своих функций и работоспособности;
- внешних воздействий (состояния внешней среды) – вероятность реализации киберугроз и размеров вреда, который может быть причинен;
- целей, интересов, возможностей всех взаимодействующих в киберпространстве сторон.

Безопасным считается такое состояние объекта, при котором кибератаки успешно блокируются системой защиты; реализованные кибератаки не достигают своей цели; в случае преодоления системы защиты, причиненный вред незначителен, не представляет опасности для структуры объекта и его функциональности.

4 Онтология кибербезопасности

Основой для построения онтологии кибербезопасности является схема, отражающая взаимосвязи основных понятий безопасности, приведенная в международном стандарте по кибербезопасности. Сформированная на этой основе онтология отражает только понятия,

описанные в данном стандарте, и лишь частично детализирует разные аспекты, которые требуется учитывать при проектировании системы обеспечения кибербезопасности объектов энергетики. Как видно из рисунка 1, для обеспечения кибербезопасности необходимо учитывать множество разнообразных факторов, отражающих особенности всех заинтересованных участников, их ресурсов, возможных угроз и принимать соответствующие меры защиты от киберопасностей.

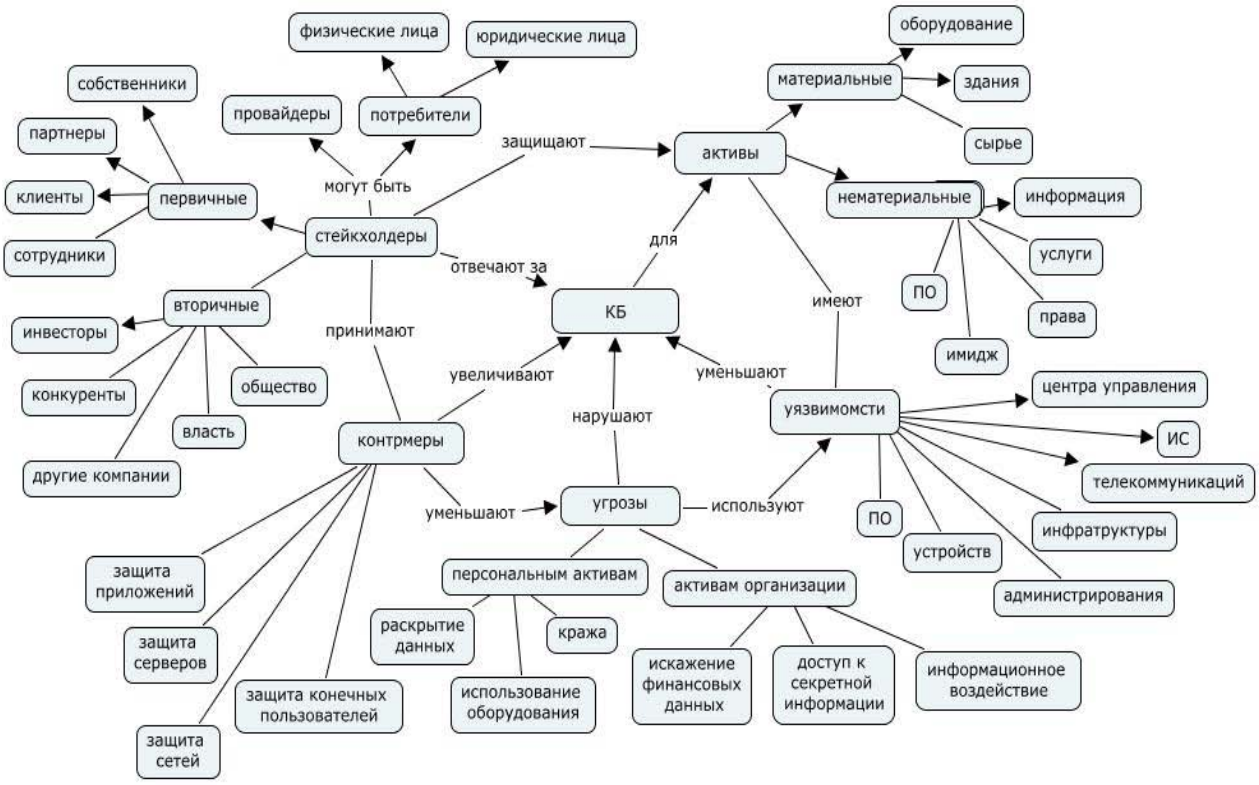

Рисунок 1 - Онтология кибербезопасности

Представленная онтология отражает только один из начальных этапов рассмотрения проблемы кибербезопасности, так как не затрагивает такие сферы, как информационная безопасность, безопасность приложений, сетей, информационных систем и другие. Для более глубокого исследования кибербезопасности систем и объектов энергетики необходима дальнейшая детализация рассмотренных понятий в их привязке к особенностям конкретных информационных систем и систем управления энергетическими объектами.

5 Основные функции системы обеспечения кибербезопасности

На основе сформированной онтологии можно спроектировать базовый прототип системы обеспечения кибербезопасности, отражающий ее основные задачи, компоненты и функции. При проектировании ИС обеспечения кибербезопасности необходимо решить несколько задач.

- Определиться с объектами защиты (активами), выявить элементы, сферы деятельности объекта, уровни управления, на которые может быть направлено воздействие.
- Сформировать источники угроз – субъекты, объекты, внутренние, внешние, естественные, искусственные, проанализировав цели и возможности всех заинтересованных участников (стейкхолдеров).

- Выполнить анализ возможных средств и методов реализации угроз, ранжировать угрозы по степени опасности (с учетом вероятности их реализации и размеров возможно причиненного ущерба).
- Предусмотреть мероприятия по противодействию угрозам (контрмеры).
- Выполнить мониторинг уязвимостей всех активов.

По аналогии с системами кибербезопасности органов военного и государственного управления [10] проектируемая ИС должна выполнять следующие функции:

- мониторинга киберпространства для обнаружения кибератак и возникновения киберугроз;
- комплексной защиты информации от несанкционированного доступа;
- противодействия кибератакам.

Мониторинг киберпространства подразумевает систематический сбор информации о возможных угрозах кибербезопасности, их источниках, времени, содержании, выявлении признаков и фактов атак, ведение базы данных с каталогом потенциальных угроз и признаков кибервоздействий на информационные ресурсы.

Комплексная система защиты информации включает контроль технических каналов связи, средства обнаружения компьютерных атак, контроль управления доступом и другие организационные и программно-технические меры.

Противодействие включает планирование и ведение упреждающих действий, активное воздействие на процесс атаки, парирование атак. Противодействие внешним угрозам может осуществляться уклонением от нападения, блокированием угроз, вплоть до уничтожения их источника; внутренним угрозам – профилактикой, локализацией источника, системой контроля и управления доступом.

При этом необходимо учитывать фактор постоянных изменений, происходящих в окружающем киберпространстве – возникновение новых киберугроз и кибератак, выявление уязвимостей и их появление, изменения в активах, подлежащих защите, цели и возможности стейкхолдеров, разработку новых средств защиты и др.

Заключение

Системы и объекты энергетики относятся к объектам критической инфраструктуры. Обеспечение их кибербезопасности невозможно без постоянного мониторинга ситуации с точки зрения возникновения угроз, выявления уязвимостей, принятия мер защиты. Невозможно обеспечить абсолютную кибербезопасность, но необходимо стремиться к достижению киберустойчивости системы.

Для оценки ситуаций, эффективного управления, принятия оперативных и стратегических решений необходимы все более развитые ИС, базирующиеся на использовании формализованных знаний соответствующей предметной области, которые и могут предоставить онтологии. Применительно к объектам энергетики разработка системы обеспечения кибербезопасности требует скоординированных усилий во всех областях компьютерных систем – прикладной, информационной, сетевой, технической, образовательной и научной.

Благодарности

Работа выполнена при финансовой поддержке гранта РФФИ № 13-07000140 «Методология создания и интеграции интеллектуальных, агентных и облачных вычислений в Smart Grid (умных энергетических системах)» и гранта Программы Президиума РАН (229)

«Методы и инструментальные средства поддержки принятия решений в исследованиях и обеспечении энергетической безопасности на основе интеллектуальных вычислений».

Список источников

[1] ***Воропай, Н.И.*** Интеллектуальные электроэнергетические системы: концепция, состояние, перспективы // Автоматизация и IT в энергетике. – №3. – 2011. – С. 11-16

[2] ***Массель, Л.В.*** Проблемы создания Smart Grid в России с позиций информационных технологий и кибербезопасности / Труды Всероссийского семинара с международным участием «Методические вопросы исследования надежности больших систем энергетики»: Вып.64. Надежность систем энергетики: достижения, проблемы, перспективы.- Иркутск: ИСЭМ СО РАН.- 2014.- С. 171-181

[3] ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity.

[4] ***Марков А.С., Цирлов В.Л.*** Руководящие указания по кибербезопасности в контексте ISO/IEC 27032. / Вопросы кибербезопасности. № 1, 2014

[5] ГОСТ 53114-2008. Обеспечение информационной безопасности организации. Основные термины и определения. http://www.pqm-online.com/standards (актуально на 15.10.2014).

[6] ГОСТ 50922-2006 Защита информации. Основные термины и определения. http://gostexpert.ru/gost/gost-50922-2006 (актуально 15.10.2014).

[7] ***Мохор В.В., Богданов А.М., Килевой А.С.*** Наставления по кибербезопасности (ISO/IEC 27032:2012) / Изложение стандарта ISO/IEC 27032:2012 «Информационные технологии. – Методы обеспечения безопасности. – Наставления по кибербезопасности».

[8] ***Атаманов, Г.А.*** Методология безопасности. Материалы и публикации о безопасности / http://www.naukaxxi.ru/materials. (актуально на 15.10.2014).

[9] ***Атаманов, Г.А.*** Диалектика безопасности. / "Национальная безопасность России в перспективах современного развития", Саратов: ООО Изд-во «Научная книга», 2005. - С. 21–27.

[10] ***Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В.*** Кибербезопасность как основной фактор национальной и международной безопасности XXI века. / Вопросы кибербезопасности № 1(2) 2014. С. 5-12

ONTOLOGY AS THE BASIS FOR THE DEVELOPMENT OF INTELLIGENT CYBERSECURITY SYSTEMS

T.N. Vorozhtsova

Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences (ESI SB RAS), Irkutsk, Russia

tnn@isem.sei.irk.ru, tnvr@yandex.ru

Abstract

This article describes the ontology cybersecurity developed on the basis of standards. The international standard ISO/IEC 27032:2012 «Information technology. Security techniques. Guidelines for cybersecurity» was used as a basis. The article discusses basic concepts related to the issue of cybersecurity and their relationship. The possibility of designing the basic structure of intelligent systems cybersecurity of energy facilities on the basis of formalized representation of these concepts and relationships is investigated.

Key words: *cyber security, ontology, information security, intelligent system, knowledge formalization*

References

[1] ***Voropai N.I.*** Intellektualnye elektroenergeticheskye sistemy: kontceptciya, sostoianiye, perspektivy [Intelligent power system: concept, status, prospects] // Avtomatizhtciya i IT v energetike. (Automation and IT in energy sector). – №3. – 2011. – P. 11-16. (In Russian).

[2] ***Massel L.V.*** Problemy sozdaniya Smart Grid v Rossii s pozitci informatcionnikh tekhnologi i kiberbezopasnosti [Problems of creation of the Smart Grid in Russia from a position of information technology and cybersecurity] //

Proceedings of all-Russian seminar with international participation «Methodological research questions the reliability of large energy systems»: V. 64. Reliability of energy systems: achievements, problems, prospects. - Irkutsk: ESI SB RAS. - 2014. - P. 171-18. (In Russian).

[3] ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity.

[4] ***Markov A.S., Tcirlov V.L.*** Rukovodiashie ukazaniya po kiberbezopasnosti v kontekste ISO/IEC 27032 [Guidance on cybersecurity in the context of ISO/IEC 27032]. / Voprosy kiberbezopasnosti (The cybersecurity). № 1, 2014 (In Russian).

[5] GOST 53114-2008. Obespechenie informatcionnoi bezopasnosti organizatcii [The information security organization]. Basic terms and definitions. http://www.pqm-online.com/standards. (In Russian).

[6] GOST 50922-2006. Informatcionnaya bezopasnost [The information security]. Basic terms and definitions. http://gostexpert.ru/gost/gost-50922-2006. (In Russian).

[7] ***Mokhor V.V., Bogdanov A.M., Kilevoi A.S***. Nastavleniya po kiberbezopasnosti. Izloshenie standarta [Guidance on cybersecurity. Standard ISO/IEC 27032:2012] / ISO/IEC 27032:2012. (In Russian).

[8] ***Atamanov G.A.*** Metodologiya bezopasnosti. Matherialy i publikatsii o bezopasnosti [Methodology security. Materials and publications on the security] / http://www.naukaxxi.ru/materials. (In Russian).

[9] ***Atamanov G.A..*** Dialectika bezopasnosti [Dialectics of security]. / "Natcionalnaiya bezopasnost Rossii v perspektivakh sovremennogo razvitiya", Saratov, Publishing house "Science Book", 2005. – p.21-27. (In Russian).

[10] ***Borodakii U.V., Dobrodeev A.U., Butusov I.V.*** Kiberbezopasnost kak osnovnoi faktor nasionalnoi i mezhdunarodnoi bezopasnosti XXI veka. / Voprosy kiberbezopasnosti [The cybersecurity] № 1(2) 2014. С. 5-12. (In Russian).

Сведения об авторах

Ворожцова Татьяна Николаевна, 1952 г. рождения. Окончила Иркутский институт народного хозяйства (ИИНХ, ныне Байкальский государственный университет экономики и права – БГУЭП) в 1975 г., к.т.н. (2008). Ведущий инженер лаборатории информационных технологий в энергетике Института систем энергетики им Л.А.Мелентьева. В списке научных трудов более 30 работ в области автоматизации научных исследований, проектирования и программирования.

Vorozhtsova Tatyana Nikolayevna (b.1952) graduated from the Irkutsk Institute of National Economy in 1975, PhD (2008). She is a leading engineer of laboratory of information technologies in the energy sector of the Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences. She is co-author more 30 scientific articles and abstracts in the field of automation of scientific research, design, and programming.

.