УДК 004.8:620.9

ОНТОЛОГИЧЕСКИЙ ИНЖИНИРИНГ ДЛЯ РАЗРАБОТКИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АНАЛИЗА УГРОЗ И ОЦЕНКИ РИСКОВ КИБЕРБЕЗОПАСНОСТИ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

А.Г. Массель[a], Д.А. Гаськова[b]

Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения РАН, Иркутск, Россия
[a] *amassel@gmail.com,* [b] *gaskovada@gmail.com*

Аннотация

В статье описываются результаты применения онтологического инжиниринга при разработке интеллектуальной системы анализа угроз и оценки рисков нарушения кибербезопасности энергетических объектов. Построено онтологическое пространство знаний проблемной области оценки рисков, включающей идентификацию, анализ и оценивание рисков инцидентов кибербезопасности, способных вызвать экстремальные ситуации в энергетике. Представлены архитектура разрабатываемой интеллектуальной системы и задачи, для решения которых выполнялся онтологический инжиниринг. Онтологическое пространство знаний представлено онтологиями, разработка которых ведётся для каждого блока интеллектуальной системы. Приводятся онтологии, отражающие основные понятия кибербезопасности, включая актуальные угрозы в энергетическом секторе, классификацию рисков и компоненты сценария возникновения экстремальной ситуации в энергетике. Разработанные онтологии позволили интегрировать понятия основных областей исследования, в числе которых энергетическая безопасность, кибербезопасность, сценарное планирование и управление рисками. В работе использованы методы системного анализа, методические основы построения интеллектуальных информационных систем в энергетике, методы поддержки принятия решений, методы инженерии знаний, включая онтологический инжиниринг. Новизна работы - в структурировании экспертных знаний и построении онтологического пространства знаний, которое используется для разработки интеллектуальной системы анализа угроз и оценки рисков нарушения кибербезопасности объектов энергетики.

Ключевые слова: *кибербезопасность, онтологический инжиниринг, энергетические объекты, интеллектуальная система.*

Цитирование: *Массель А.Г.* Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов / А.Г. Массель, Д.А. Гаськова // Онтология проектирования. – 2019. – Т.9, №2(32). – С. 225-238. – DOI: 10.18287/2223-9537-2019-9-2-225-238.

Введение

Распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р утверждена программа «Цифровая экономика Российской Федерации». Цифровая энергетика развивается с учётом федеральных стратегий и отраслевых программ [1]. При этом цифровизация объектов энергетики (ОЭ) может вызывать возникновение киберугроз, связанных с внедрением новых решений, применением новых бизнес-моделей, которые сопровождаются отсутствием или недостаточностью информации для оперативного принятия решений по обеспечению безопасности объекта. В связи с этим необходимо расширять область знаний об объектах, рассматривать взаимосвязи технологических процессов на ОЭ и их влияние на состояние энергетической безопасности как самого объекта, так и внешней среды. Энергетическая безопасность рассматривается как состояние защищённости страны, её граждан, обще-

ства, государства, экономики от угроз дефицита в обеспечении их потребностей в энергии экономически доступными топливно-энергетическими ресурсами приемлемого качества в нормальных условиях и при чрезвычайных обстоятельствах, а также от нарушений стабильности, бесперебойности топливо- и энергообеспечения [2]. Эти угрозы определяются как внешними (геополитическими, макроэкономическими, конъюнктурными) факторами, так и состоянием и функционированием энергетического сектора страны [3]. В последнее время список угроз расширен угрозами кибербезопасности, реализация которых может спровоцировать экстремальные ситуации в энергетике, чреватые значительным снижением возможностей обеспечения энергоресурсами потребителей. Киберугрозы рассматриваются как один из важнейших современных видов угроз энергетической безопасности [4].

Применение онтологического инжиниринга для систематизации основных понятий предметной области (ПрО) может связать все виды угроз, их взаимовлияния друг на друга и на остальные концепты ПрО.

Понятие онтологического инжиниринга относится к инженерии знаний – разделу инженерной деятельности, направленной на использование знаний в компьютерных системах для решения сложных задач [5]. Целями онтологического инжиниринга являются повышение уровня интеграции информации, необходимой для принятия управленческих решений, повышение эффективности информационного поиска, предоставление возможности совместной обработки знаний на основе единого семантического описания пространства знаний.

В энергетическом секторе широко применяется онтологический инжиниринг для поддержки принятия стратегических решений, обеспечивающий взаимосвязи и согласованность исследований при разработке систем онтологий. Система онтологий, включающая онтологии ситуационного управления, а также методика проведения исследований стратегий развития энергетики представлена в работе [6]. В работе [7] онтология топливно-энергетического сектора (ТЭК) применяется при моделировании критических инфраструктур энергетики. Формальное описание отраслей энергетики и компонентов интеллектуальной системы (ИС) поддержки принятия стратегических решений применяется в исследованиях энергетической безопасности [8, 9]. При разработке системы оперативного мониторинга технологической инфраструктуры нефтегазодобывающих предприятий применялся формат представления данных в виде объектов онтологии [10]. Исследование кибербезопасности и её основные понятия в соответствии с ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности», а также основные особенности кибербезопасности в энергетике изложены в работе [11].

1 Применение онтологий при разработке ИС

С целью исследования возможных обстоятельств нарушения энергетической безопасности, вызванных реализацией киберугроз, авторами разрабатывается ИС анализа угроз и оценки рисков нарушения кибербезопасности ОЭ [12]. Общая архитектура ИС представлена на рисунке 1 и включает:

- экспертную систему (ЭС) «Cyber» - продукционная ЭС, предназначенная для сопровождения аудита безопасности на энергетическом предприятии и выявления типовых уязвимостей, угроз и векторов атак информационно-технологической системы (ИТС) объекта;
- блок Байесовских сетей доверия (БСД), предназначенный для моделирования экстремальной ситуации, вызванной нарушением кибербезопасности, и определения вероятности наступления последствий;
- блок оценки рисков последствий от реализации киберугроз, включающий ранжирование активов и ОЭ в соответствии с величиной риска и критериев ранжирования.

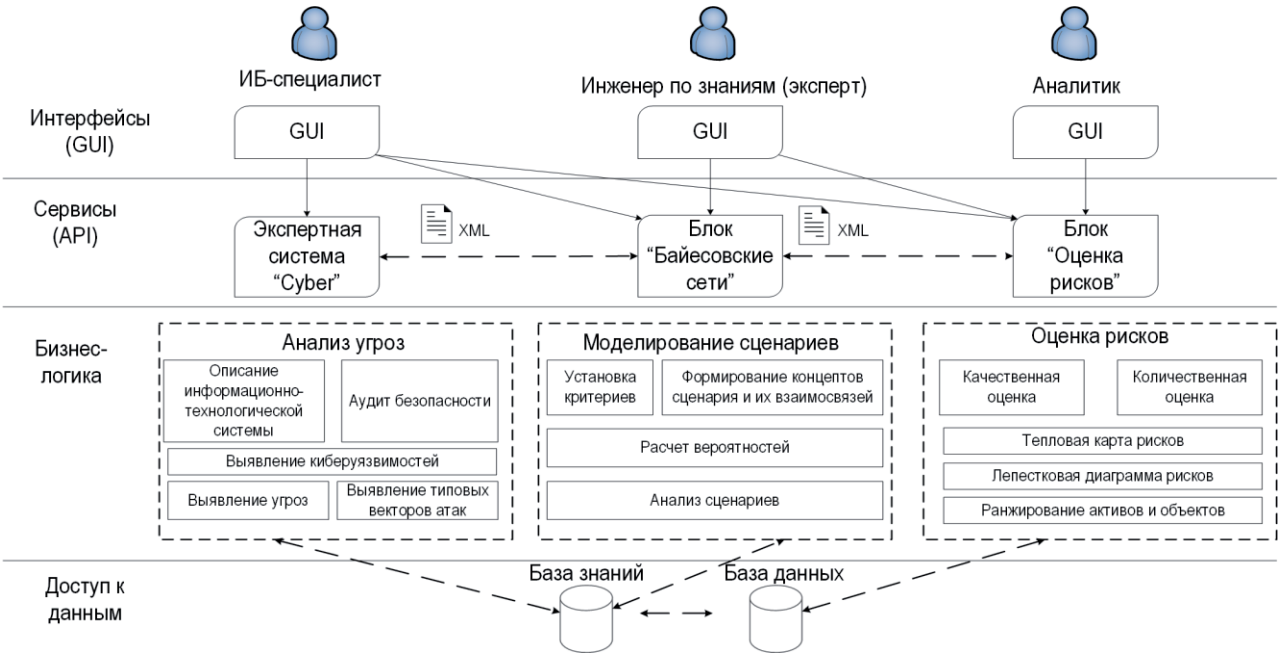

Рисунок 1 – Архитектура ИС анализа угроз и оценки рисков нарушения кибербезопасности ОЭ

Разработка ИС основана на методике анализа угроз и оценки рисков (АУОР) нарушения информационно-технологической безопасности энергетических комплексов [13], переработанной для ОЭ и дополненной аспектами кибербезопасности. ИС разрабатывается для решения следующих групп задач:

- анализ киберугроз;
- моделирование сценариев;
- оценивание рисков, включающих ранжирование объектов и их активов.

Под анализом киберугроз понимается комплекс мероприятий по идентификации риска, включающий подготовку к анализу угроз и риска, в том числе установление контекста менеджмента риска, сбор и анализ данных, установление границ АУОР, а также предварительную оценку критичности активов рассматриваемого объекта. Для реализации последнего посредством ЭС «Cyber» предлагается провести аудит безопасности ИТС объекта в форме анкетирования, на основе чего определяется список предполагаемых активов, содержащих уязвимости, а также вероятные (тривиальные) угрозы.

В качестве критериев для составления анкет и проведения анкетирования предлагается использовать известные векторы атак реализации киберугроз. Выделены два основных направления векторов атак на промышленные компании: нецелевые атаки, направленные на IT-инфраструктуру, воздействие на которую может негативно повлиять на штатное функционирование промышленных систем; целевые атаки, направленные на промышленное оборудование. В первом случае рассматривается проникновение в корпоративную сеть и получение доступа к локальной вычислительной сети. Во втором - проникновение из корпоративной сети в технологическую и развитие атаки до получения доступа к критически важным системам [14].

Моделирование сценариев осуществляется в разрабатываемом блоке Байесовских сетей, который предназначен для анализа риска. Эта группа задач включает построение графа, отражающего вероятностные взаимосвязи между идентифицированными уязвимостями активов, угрозами, средствами контроля и последствиями. Ситуацию на объекте, например, нормальное функционирование, критическая или чрезвычайная ситуация, предлагается опреде-

лять вероятностным интегральным показателем, который является потомком всех узлов последствий, основанным на индикативном анализе.

Для оценивания рисков разрабатывается блок оценки рисков, который включает качественное и количественное оценивание рисков инцидентов безопасности, приводящих к экстремальным ситуациям в энергетике.

Риски определяются тройкой:

(1) $$R = \{T, V, D\},$$

где T – угрозы, V – уязвимости, D – ущерб при реализации угрозы.

Оценивание рисков включает три основных процесса:

- описание рисков всех значимых сценариев в соответствии с классификацией;
- измерение уровня риска, в процессе которого присваиваются качественные значения критичности и последствий риска;
- количественное измерение уровня риска основывается на байесовской вероятности наступления последствий и оценке возможного ущерба в денежном эквиваленте.

Группа задач ранжирования объектов и их активов связана с определением критических активов на основе величины риска внутри объекта, а также определением ОЭ, наиболее подверженных рискам наступления экстремальных ситуаций за счёт реализации киберугроз.

Величина риска внутри объекта определяется как:

(2) $$R_o = \{T_o, V_o, D_o\},$$

где T_o – совокупность угроз, V_o – совокупность уязвимостей активов на объекте, D_o – сумма ущербов при реализации угрозы.

Для решения этих задач разрабатывается одноименный блок ИС.

Онтология задач (нижний уровень) и реализующих их блоков ИС (верхний уровень) представлена на рисунке 2.

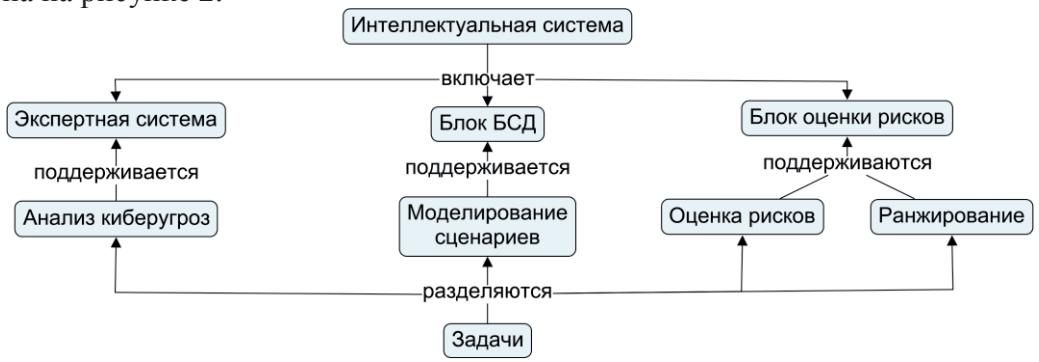

Рисунок 2 – Онтология задач и инструментальных средств анализа угроз и оценки рисков нарушения кибербезопасности ОЭ

При проектировании системной архитектуры ИС необходимо решить задачи классификации основных понятий, установления взаимосвязей между ними, выявления основных процессов и методов, применяемых при оценке рисков кибербезопасности, а также структуризации знаний по анализу угроз и оценке рисков нарушения кибербезопасности ОЭ. Для решения этих задач была разработана система онтологий для каждого блока ИС.

2 Онтологическое пространство знаний ИС анализа угроз и оценки рисков

Онтологическое пространство знаний, представляющее собой систему онтологий, логически объединённых по каждому разделу ПрО, представлено на рисунке 3. Система онтологий включает онтологии, отражающие основные концепты разделов ПрО и их взаимосвязи. В качестве разделов ПрО выступают анализ киберугроз, включая предварительную подго-

товку и результирующую модель угроз; вероятностные сценарии, с учётом анализа угроз; оценка рисков, с учётом последствий наступления экстремальных ситуаций, и выявление критически значимых активов ОЭ.

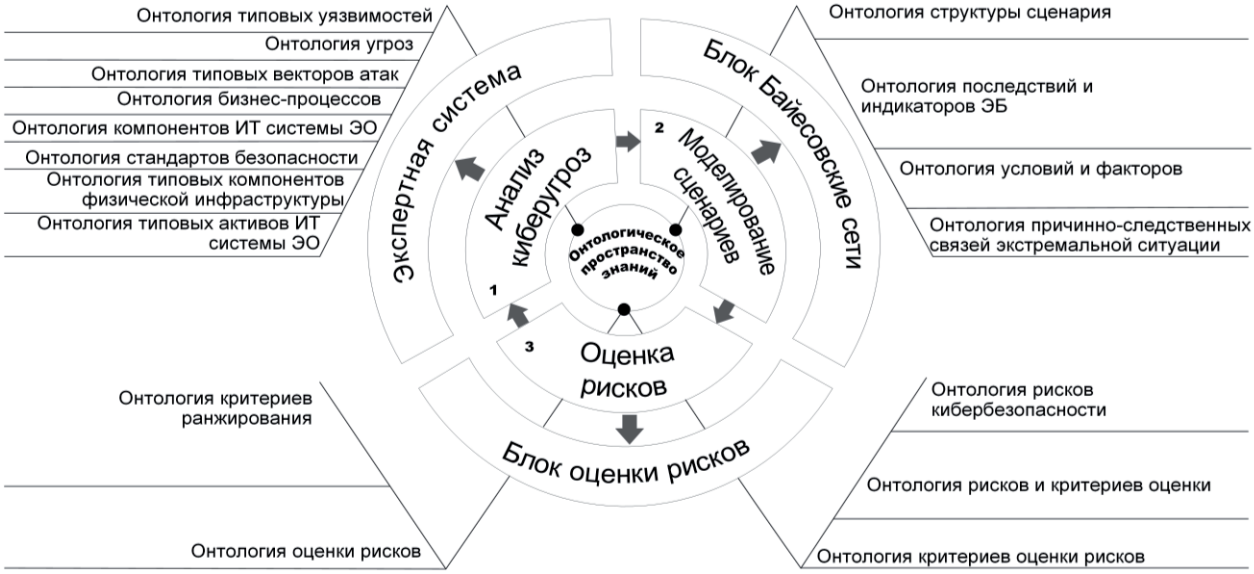

Рисунок 3 – Онтологическое пространство знаний для разработки ИС анализа угроз и оценки рисков нарушения кибербезопасности ОЭ

2.1 Анализ киберугроз

Анализ угроз до сих пор остаётся нетривиальной задачей. Наибольшая сложность заключается в сопоставлении уязвимостей активов информационно-технологических (ИТ) систем, используемых на предприятии, и возможных угроз безопасности, реализация которых повлечёт ощутимые потери для рассматриваемого объекта. Разрабатываемая онтология для анализа угроз представлена на рисунке 4 и включает восемь взаимосвязанных онтологий.

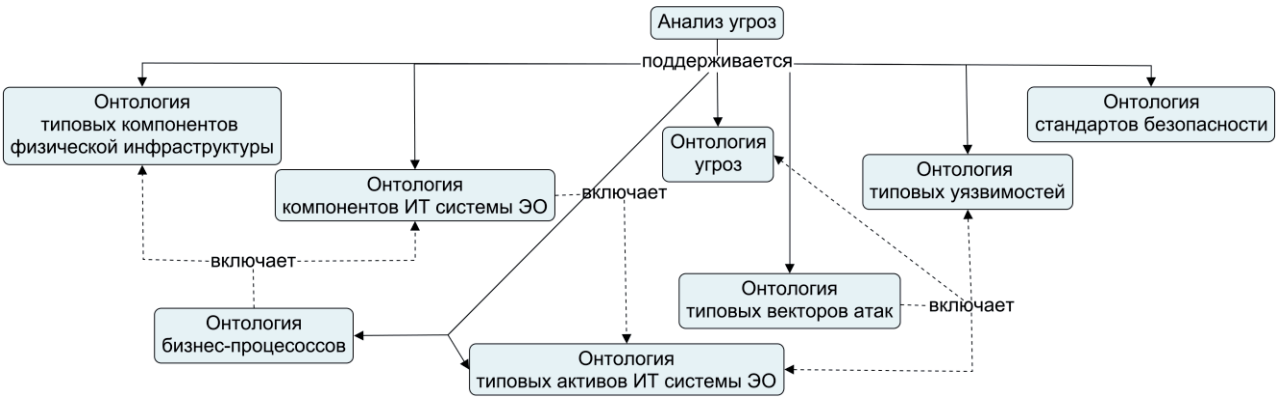

Рисунок 4 – Онтология анализа угроз

В настоящее время не существует единого нормативно-правового пространства, охватывающего вопросы обеспечения безопасности в области энергетики. Нормативные документы охватывают различные области безопасности и используют различную терминологию. Анализ нормативных документов, в том числе международных, отражен, например, в работах [15, 16]. Онтология стандартов безопасности разрабатывается с целью кластеризации знаний по методам проведения оценки безопасности, а также методам обеспечения безопасности

для каждой из областей кибербезопасности: безопасности приложений, информационной безопасности, сетевой безопасности, безопасности Интернет и защите ключевых информационных систем объектов критических инфраструктур [17]. Разрабатываемую онтологию стандартов планируется применять при составлении анкеты для проведения аудита безопасности с использованием ЭС «Cyber» [18].

С целью определения основных угроз в энергетике, связанных с нарушением кибербезопасности на объектах, разработана онтология угроз, представленная на рисунке 5. Уязвимости и угрозы содержатся в базах данных, например, «Банк данных угроз безопасности информации» ФАУ «ГНИИИ ПТЗИ ФСТЭК России» [19], международная база данных уязвимостей «Common Vulnerabilities and Exposures» (CVE) [20]. Их описания включают слабые места конкретного программного продукта. Основные задачи онтологического инжиниринга в данной области заключаются в установлении актуальных уязвимостей и угроз для энергетики и их классификации для типовых компонентов и активов ИТС. Соответствующие онтологии разрабатываются для формирования структуры и дальнейшего наполнения базы знаний ЭС «Cyber» с целью автоматизации проведения аудита безопасности на предприятии.

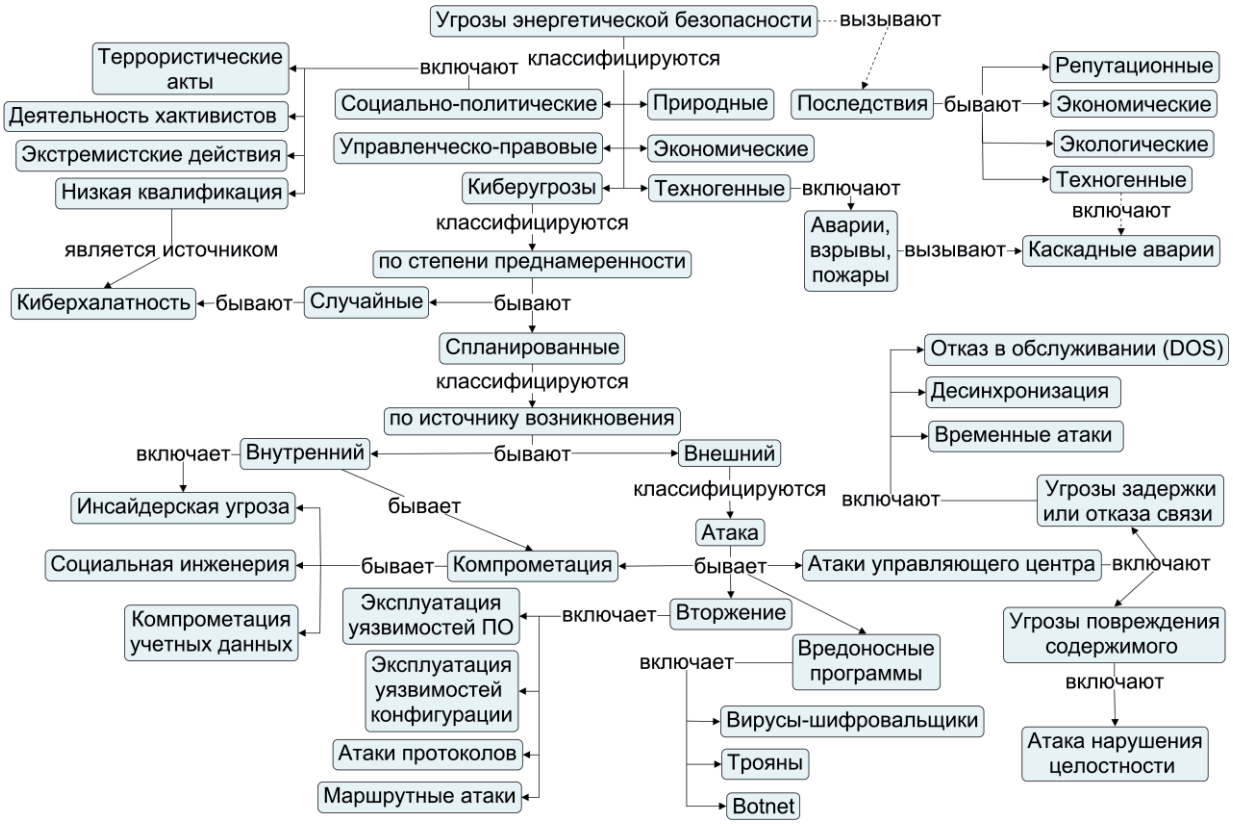

Рисунок 5 – Онтология угроз энергетической безопасности

Связи между уязвимостями и угрозами устанавливаются путём формирования векторов атак. Типовые векторы атак на промышленные предприятия и корпоративные информационные системы описаны в исследованиях ведущих компаний, таких как Лаборатория Касперского [21] и Positive Technologies [14, 22], типовые угрозы в энергетике описаны в [23]. Векторы атак в ИС описываются в виде продукционных правил, в соответствии с которыми строится граф для определения вероятности наступления экстремальных ситуаций в ОЭ.

В ходе аудита безопасности анализируются активы ИТС рассматриваемого объекта и выявляются критически значимые и содержащие уязвимости. Онтологический инжиниринг в данной области проводился на трёх уровнях автоматизированной системы управления тех-

нологическими процессами. Особое внимание при этом уделялось верхнему уровню диспетчерского управления, поскольку характерной особенностью последствий реализации угроз на данном уровне является возможность получения административного доступа к системе управления предприятием. Полученная онтология применяется при разработке анкеты для проведения аудита безопасности предприятия.

Анализ киберугроз ведётся на основе онтологического инжиниринга основных бизнес-процессов ИТС ОЭ, целью которого является обоснование полноты выявляемых уязвимостей. Для формирования базы данных об ОЭ выполняется онтологический инжиниринг типовых компонентов их физической инфраструктуры, а также компонентов ИТС, под которыми понимаются автоматизированные информационные системы, использующиеся на предприятиях энергетики.

Онтологический инжиниринг в рамках анализа угроз позволил систематизировать разрозненную информацию об ОЭ, их характеристиках и компонентах, бизнес-процессах, активах, связанных с ними уязвимостях и угрозах нарушения кибербезопасности, а также стандартах безопасности, применимых в энергетическом секторе. Представленные онтологии применяются в разрабатываемой ЭС в части формирования структуры самого компонента и базы знаний, алгоритма проведения аудита безопасности, и в дальнейшем при вероятностном моделировании сценариев.

2.2 Моделирование сценариев экстремальных ситуаций в энергетике

Задачи по прогнозированию условий функционирования и развития систем энергетики и ТЭК, оценке их состояния, выбор альтернатив и мер по предотвращению критических и чрезвычайных ситуаций в энергетике решаются в рамках модельных сценарных исследований [7]. При решении задачи прогнозирования поведения ОЭ в условиях нарушения кибернетической безопасности, вызывающих реализацию угроз энергетической безопасности (ЭБ), проводился онтологический инжиниринг, по результатам которого сформирована система онтологий, представленная на рисунке 6.

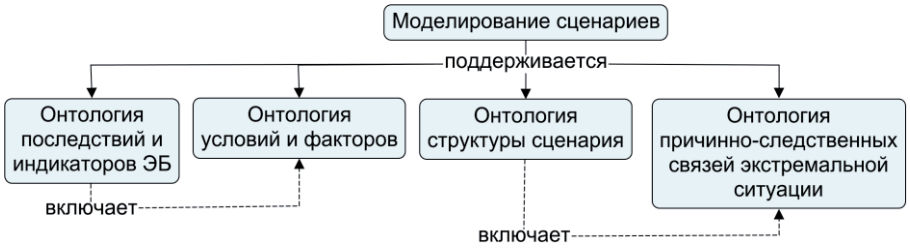

Рисунок 6 – Онтология экстремальных ситуаций в энергетике

Количество инцидентов, связанных с реализацией киберугроз на промышленных предприятиях, растет [14], а возглавляет список энергетический сектор [21]. На основе онтологии экстремальных ситуаций в энергетике, вызванных киберугрозами, определены структура ИС, блоки БСД и оценки рисков.

Построение сценариев в ИС осуществляется в блоке БСД. Такие блоки хорошо зарекомендовали себя в качестве инструмента вероятностного моделирования для анализа как угроз ЭБ [24], так и экономических рисков [25] и рисков информационных технологий [26].

Для построения бизнес-логики блока БСД разработана онтология сценария экстремальной ситуации в энергетике, вызванной нарушением кибербезопасности на объекте. Рисунок 7 демонстрирует основные концепты сценария, их характеристики и взаимосвязи. Сценарий экстремальной ситуации в энергетике представляет собой вероятностные оценки возможных ситуаций, представленные последовательностью уязвимостей, киберугроз, угроз энергетиче-

ской безопасности и угрозами причинения ущерба рассматриваемому предприятию и/или территориально-приближенной внешней среде либо энергосистеме в целом, а также пессимистические оценки основных количественных характеристик исследуемых ОЭ в условиях нарушения кибербезопасности рассматриваемого объекта [27].

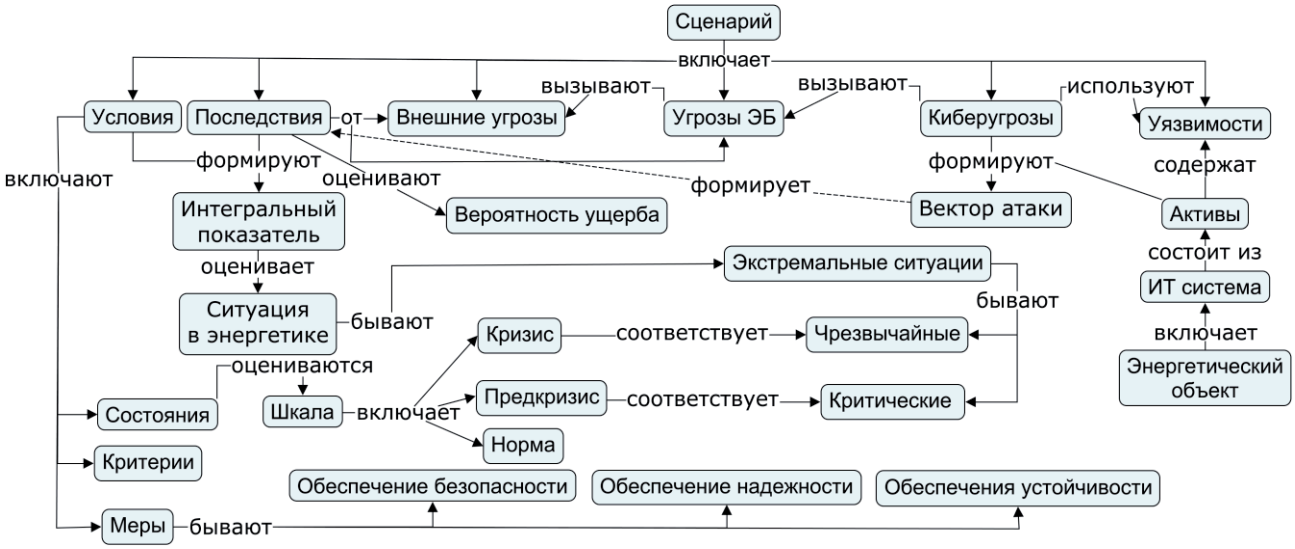

Рисунок 7 – Онтология сценария экстремальной ситуации в энергетике, вызванной киберугрозами

Помимо присутствия уязвимостей в активах ИТС или отсутствия средств защиты и методов обеспечения надежности, немаловажными при возникновении той или иной ситуации являются текущее состояние системы и влияющие на неё факторы, например, такие, как сезонность, экологическая значимость прилегаемой территории, социальные факторы и другие. Это направление онтологического инжиниринга основывается на исследованиях устойчивости энергетических систем [28, 29] и их технологической безопасности [30].

В процессе формирования графа экстремальной ситуации оценивается вероятность наступления некоторых негативных событий, таких, как падение мощности, снижение нагрузки, отключение групп потребителей и др. В работах по исследованию ЭБ разработаны индикаторы, по которым можно судить о наступлении той или иной экстремальной ситуации [2]. В этом направлении разрабатывается онтология последствий и индикаторов ЭБ на основе анализа описанных инцидентов, например [31, 32].

2.3 Оценки рисков

Процесс оценки рисков включает в себя два этапа: анализ рисков и оценивание рисков. Анализ рисков сопровождается идентификацией значимых угроз и уязвимостей, а также оценкой вероятности реализации угроз и уязвимостей [33].

Анализ рисков проводится в рамках решения задач по анализу киберугроз и моделированию сценариев экстремальных ситуаций в энергетике. Для решения задачи по оцениванию рисков применяется онтологический инжиниринг в области управления рисками, результаты которого представлены на рисунке 8.

Риск рассматривается как сочетание последствий некоторого события (инцидента) и связанной с ним возможностью возникновения (вероятностью), а оценка рисков – как процесс идентификации, анализа и оценивания, в соответствии с международным стандартом ISO/IEC 27005:2011 «Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности».

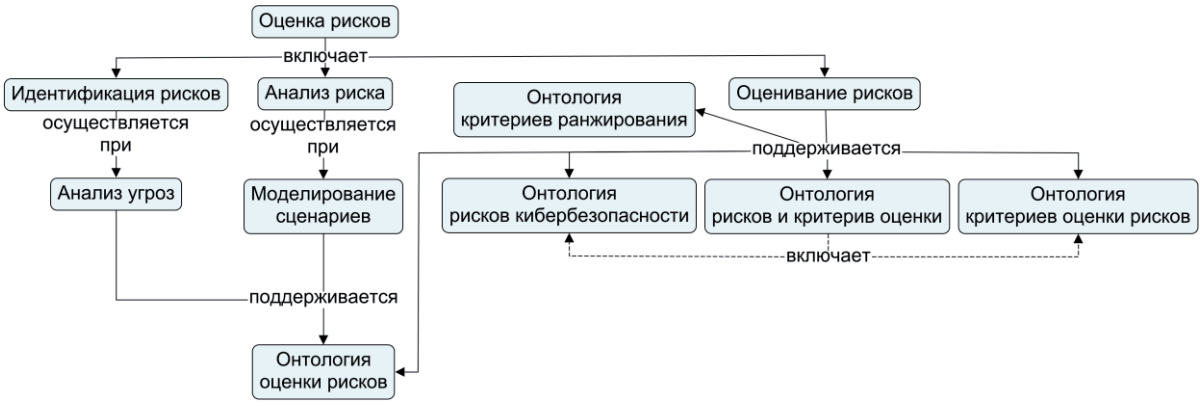

Рисунок 8 – Онтология оценки рисков нарушения кибербезопасности ОЭ

Риски кибербезопасности рассматриваются, с одной стороны, как риски киберсреды, а с другой - как вид рисков ЭБ, связанных с нарушением функционирования физической инфраструктуры ОЭ, приводящим к негативным последствиям. Онтология рисков кибербезопасности в энергетике представлена на рисунке 9.

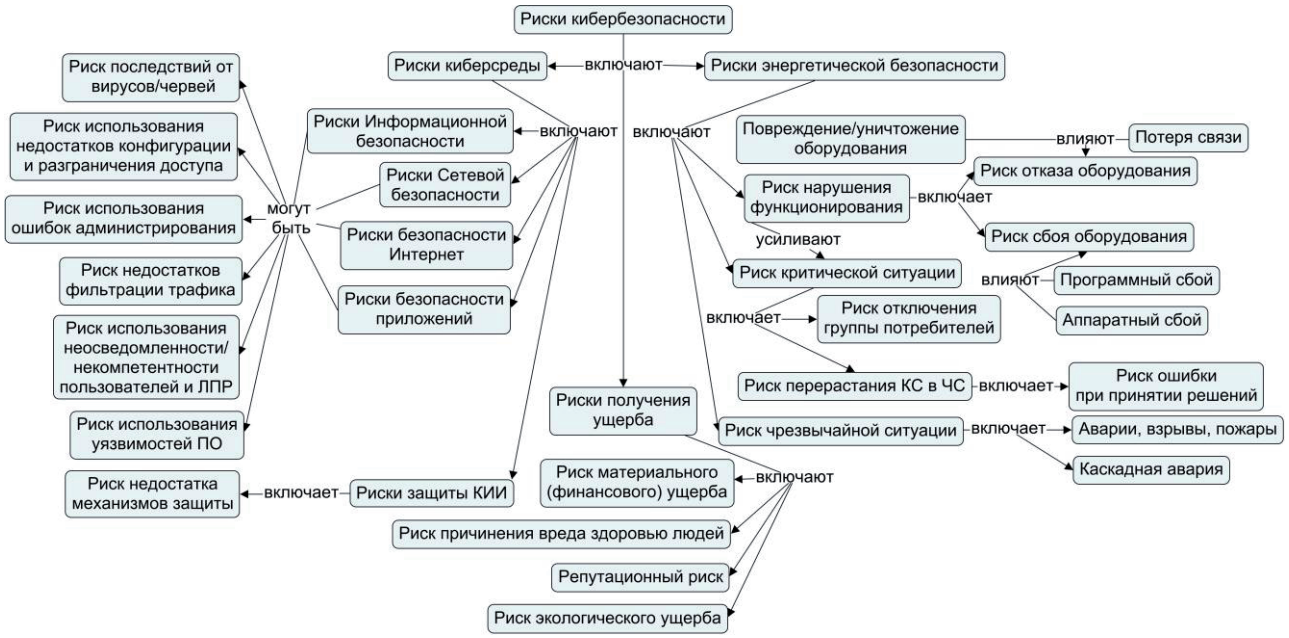

Рисунок 9 – Онтология рисков кибербезопасности в энергетике

Основные критерии оценки рисков отражены в законе от 26 июля 2017 года № 187-ФЗ «О защите критической информационной инфраструктуры Российской Федерации». На основе данного закона разработана онтология критериев оценивания рисков.

Оценка рисков основывается главным образом на стандарте ISO/IEC 27005, а также методике АУОР [13]. На заключительном этапе оценки рисков предлагается проводить ранжирование объектов. Для этого вводится критерий значимости объекта:

$$K_S = \{C, R, F\},$$

где K_S – критерий значимости; C – критерий оценки рисков, R – интегральный показатель рисков объекта, F– объект, представленный совокупностью основных характеристик.

Критерии оценки рисков складываются из оценки влияния на технологическую, экологическую или социальную составляющую рисков, в зависимости от того, какой фактор более важен (определяется экспертным путём). Интегральный показатель рисков объекта склады-

вается из формулы (2). В качестве F принимают основные характеристики ОЭ, например производственная мощность. Объектам выставляются ранги согласно оценке показателя критерия значимости. Пользователь определяет проранжированый список ОЭ с учётом критерия значимости и величины рисков наступления экстремальной ситуации при возникновении киберугроз на каждом из объектов.

Заключение

Рассмотрены ПрО анализа угроз и оценки рисков нарушения кибербезопасности в энергетике. Применение онтологического инжиниринга позволило структурировать знания экспертов и данные стандартов в области безопасности. Приведены онтологии, использованные при разработке ИС анализа угроз и оценки рисков нарушения кибербезопасности ОЭ, объединенные в онтологическое пространство знаний ПрО. Дано описание взаимосвязей онтологий и показано их применение в ИС.

Благодарности

Результаты получены в рамках выполнения госзадания ИСЭМ СО РАН № АААА-А17-117030310444-2, а также в рамках проектов, поддержанных грантами РФФИ № 19-07-00351, Бел_мол_а № 19-57-04003, № 18-07-00714, мол_а № 18-37-00271, № 17-07-01341.

Список источников

[1] ***Массель, Л.В.*** Методы и интеллектуальные технологии научного обоснования стратегических решений по цифровой трансформации энергетики / Л.В. Массель // Энергетическая политика. № 5. 2018. – С.30-42.

[2] Энергетическая безопасность России: проблемы и пути решения / Н.И. Пяткова, В.И. Рабчук, С.М. Сендеров, М.Б. Чельцов. Новосибирск: СО РАН, 2011. - 198 с.

[3] Энергетическая безопасность России // Н.И. Воропай, С.М. Сендеров, Н.И. Пяткова, Г.Б Славин. Новосибирск: Наука, 1998. - 302 с.

[4] ***Массель, Л.В.*** Киберопасность как одна из стратегических угроз энергетической безопасности / Л.В. Массель, Н.И. Воропай, С.М. Сендеров, А.Г. Массель // Вопросы кибербезопасности. № 4 (17). 2016. – С.2-10.

[5] ***Гаврилова, Т.А.*** Инженерия знаний. Модели и методы. / Т.А. Гаврилова, Д.В. Кудрявцев, Д.И. Муромцев. — СПб.: Издательство «Лань», 2016. — 324 с.

[6] ***Массель, Л.В.*** Онтологический инжиниринг для поддержки принятия стратегических решений в энергетике / Л.В. Массель, Т.Н. Ворожцова, Н.И. Пяткова // *Онтология проектирования*. – 2017. – Т. 7, № 1(23). – С.66-76. – DOI: 10.18287/2223-9537-2017-7-1-66-76.

[7] ***Пяткова, Н.И.*** Моделирование критических инфраструктур энергетики с учетом требований энергетической безопасности / Н.И. Пяткова, Н.М. Береснева // Информационные и математические технологии в науке и управлении. - 2017. № 3(7).– С.54-65.

[8] ***Ворожцова, Т.Н.*** Онтологическая модель пространства знаний для ситуационного управления в энергетике / Т.Н. Ворожцова // XX Байкальская Всероссийская конференция «Информационные и математические технологии в науке и управлении»: труды. Т. 3. Иркутск. ИСЭМ СО РАН. 2015. - С.85-88.

[9] ***Копайгородский, А.Н.*** Применение онтологий в семантических информационных системах / А.Н. Копайгородский // Онтология проектирования. – № 4 (14). – 2014. – С.78-89.

[10] ***Загорулько, Ю.А.*** Онтологический подход к разработке системы поддержки принятия решений на нефтегазодобывающем предприятии / Ю.А. Загорулько, Г.Б. Загорулько // Вестник НГУ. Серия: Информационных технологии. Том 10, Выпуск 1. 2012. – С.121-128.

[11] ***Ворожцова, Т.Н.*** Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности / Т.Н. Ворожцова // Онтология проектирования. – № 4 (14). – 2014. – С.69-77.

[12] ***Gaskova, D.*** Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility / D. Gaskova, A. Massel // Proceedings of the 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC). Vladivostok. Publisher: IEEE. – 2018. – P.1-5.

[13] ***Массель, А.Г.*** Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов / А.Г. Массель // XX Байкальской Всероссийской конференции: труды, т. III. – Иркутск: ИСЭМ СО РАН, 2015. – С.186-195.

[14] Positive Technologies Промышленные компании: векторы атак. 23 апреля 2018. - 24 с. - https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/.

[15] ***Юдин, А.*** Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности Smart Grid систем / А. Юдин, Г. Пирогов // Научно-технический сборник «КПИ им. Игоря Сикорского» «Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине». Выпуск 25. – 2013. – С.88-95.

[16] ***Литвинов, П.*** Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищённости и оптимизации затрат / П. Литвинов // Портал «Мир компьютерной автоматизации». – http://www.rtsoft.ru/press/23432/imitatsionnoe-modelirovanie-voprosov-informatsionnoy-bezopasnosti-kak-instrument-otsenki-zashchishch/.

[17] Наставления по кибербезопасности (ISO/IES 27032:2012): излож. стандарта ISO/IES 27032:2012 «Информационные технологии. - Методы обеспечения безопасности. - Наставления по кибербезопасности» // В.В. Мохор, А.М. Богданов, А.С. Килевой. - Киев: Три-К, 2013. - 129 с.

[18] ***Гаськова, Д.А.*** Разработка экспертной системы для анализа угроз кибербезопасности в энергетических системах / Д.А. Гаськова, А.Г. Массель // Информационные и математические технологии в науке и управлении. - 2016. - №1. – С.113-122.

[19] Банк данных угроз безопасности информации. ФАУ «ГНИИИ ПТЗИ ФСТЭК России». - https://bdu.fstec.ru/.

[20] Международная база данных уязвимостей Common Vulnerabilities and Exposures (CVE). - https://cve.mitre.org.

[21] WannaCry в промышленных сетях: работа над ошибками. – https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/.

[22] Positive Research 2018. Сборник исследований по практической безопасности. АО «Позитив Текнолоджиз». 2018. - 204 с. – https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf.

[23] ***Sridhar, S.*** Cyber-physical system security for the electric power grid / S. Sridhar, A. Hanh, M. Govindarasu // Proc. IEEE. 2012. Vol. 100. No. 1. – P. 210-224.

[24] ***Массель, Л.В.*** Применение байесовских сетей доверия для интеллектуальной поддержки исследований проблем энергетической безопасности / Л.В. Массель, Е.В. Пяткова // Вестник ИрГТУ. – № 2. – 2012. – С. 8-13.

[25] ***Мусина, В.Ф.*** Байесовские сети доверия как вероятностная графическая модель для оценки экономических рисков / В.Ф. Мусина // Труды СПИИРАН. Выпуск 25. – 2013. - С.235-254.

[26] ***Dantu, R.*** Risk management using behavior based Bayesian networks / R. Dantu, P. Kolan // Intelligence and Security Informatics. 2005. – P.165-184.

[27] ***Massel, A.G.*** Scenario approach for analyzing extreme situations in energy from a cybersecurity perspective / A.G. Massel, D.A. Gaskova // Industry 4.0, 2018, Issue 5. Publisher: Scientific Technical Union of Mechanical Engineering “Industry 4.0”. – P. 266-269.

[28] ***Kolosok, I.*** Cyber Resilience of SCADA at the Level of Energy Facilities / I. Kolosok, E. Korkina // Proceedings of the Vth International workshop “Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security” (IWCI 2018). 2018. - P.100-105.

[29] ***Zio, E.*** Challenges in the vulnerability and risk analysis of critical infrastructures / E. Zio // Reliability Engineering and System Safety. N 152. 2016. – P.137–150.

[30] ***Махутов, Н.А.*** Обеспечения безопасной эксплуатации объектов техносферы и населения с использованием критериев риска / Н.А. Махутов, М.М. Гаденин // Тезисы докладов XXI Междунар. научно-практ. конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. – 2016. – С.137-146.

[31] ***Массель, Л.В.*** Экспертная система Advice для выбора управляющих воздействий в ситуационном управлении в энергетике / Л.В. Массель, А.Г. Массель, А.Ю. Мякотина // Тр. XX Байкальской Всерос. конф. «Информационные и математические технологии в науке и управлении». – Иркутск: ИСЭМ СО РАН, 2015. 29 июня-07 июля 2015. – С.132-138.

[32] ***Багрова, Л.А.*** Опасные техногенные катастрофы в энергетике как факторы экологического риска / Л.А. Багрова, В.А. Боков, А.С. Мазинов // Ученые записки Таврического национального университета им. В.И. Вернадского. Серия "География". Том 25 (64). 2012 г. No2. - С.9-19.

[33] Семь безопасных информационных технологий / А.В. Барабанов, А.В. Дорофеев, А.С. Марков, В.Л. Цирлов // Под ред. А.С. Маркова. – М.: ДМК Пресс, 2017. – 224 с.

ONTOLOGICAL ENGINEERING FOR THE DEVELOPMENT OF THE INTELLIGENT SYSTEM FOR THREATS ANALYSIS AND RISK ASSESSMENT OF CYBERSECURITY IN ENERGY FACILITIES

A.G. Massel[a], D.A. Gaskova[b]

Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia
[a]amassel@gmail.com, [b]gaskovada@gmail.com

Abstract

The article describes the main results of applying ontological engineering in the development of the intelligent system for threats analysis and risk assessment of cybersecurity violations in energy facilities. The ontological knowledge space for the problem area of risk assessment has been built, comprising identification, analysis and evaluation of the risk of cybersecurity incidents that can cause extreme situations in the energy sector. The paper highlights the intellectual system architecture being developed and tasks for which the ontological engineering was carried out. The ontological knowledge space is represented as combining ontology subsystems, the development of which is carried out for each block of the intelligent system. The authors provide ontologies that reflect the basic concepts of cybersecurity, including current threats in the energy sector, risk classification and components of the emergency situation scenario in the energy sector. The produced ontologies allowed to integrate the concepts of the main research areas, including energy security, cybersecurity, scenario planning, and risk management. We used methods of system analysis, methodological foundations for building intelligent information systems in energy research, methods for supporting decision-making, methods of knowledge engineering, methods of semantic modeling, including ontological engineering. The novelty of the work is in the structuring of expert knowledge and the construction of the ontological knowledge space, which is used to develop an intelligent system for analyzing threats and assessing the risks to the cybersecurity of energy facilities.

Keywords: *cybersecurity, ontological engineering, energy facilities, intelligent system.*

Citation: *Massel A.G., Gaskova D.A.* Ontological engineering for the development of the intelligent system for threats analysis and risk assessment of cybersecurity in energy facilities [In Russian]. *Ontology of designing*. 2019; 9(2): 225-238. – DOI: 10.18287/2223-9537-2019-9-2-225-238.

Acknowledgment

This work was performed within the framework of project according to state assignment ESI SB RAS №AAAA-A17-117030310444-2. The study of separated aspects was supported by RFBR grants № 19-07-00351, № 19-57-04003, № 18-07-00714, № 18-37-00271, № 17-07-01341.

References

[1] ***Massel LV.*** Methods and intelligent technologies for scientific substantiation of strategic solutions on digital transformation of energy industry [In Russian]. Energy Policy. 2018; 5: 30-42.

[2] ***Pyatkova NI, Rabchuk VI, Senderov SM, Cheltsov MB.*** Energy Security in Russia: Problems and Solutions [In Russian]. Novosibirsk: SB RAS, 2011, p. 198.

[3] ***Voropai NI, Senderov SM, Pyatkova NI, Slavin GB***. Energy Security of Russia [In Russian]. Novosibirsk: Nauka, 1998, 302 p.

[4] ***Massel LV, Voropai NI, Senderov SM, Massel AG***. Cyber Danger as one of the strategic threats to energy security [In Russian]. Cybersecurity issues 2016; 4(17): 2-10.

[5] ***Gavrilova TA. Kudryavcev DV, Muromcev DI***. Knowledge Engineering. Models and methods [In Russian]. – SPb.: "Lan" publ., 2016, 324 p.

[6] ***Massel LV, Vorozhtsova TN, Pjatkova NI***. Ontology engineering to support strategic decision-making in the energy sector [In Russian]. Ontology of designing. 2017; 7(1): 66-76. – DOI: 10.18287/2223-9537-2017-7-1-66-76.

[7] ***Pjatkova NI, Beresneva NM***. Modeling of critical energy infrastructures taking into accont energy security [In Russian]. Information and mathematical technologies in science and management 2017; 3(7): 54-65.

[8] ***Vorozhtsova TN***. The ontological model of knowledge space for situational management in the energy [In Russian]. Proc. of the XX Baikal All-Rus. Conf. "Information and mathematical technologies in science and management". – Irkutsk. MESI SB RAS; 2015; Vol. 3: 85 - 88.

[9] ***Kopajgorodskij AN.*** The use of ontologies in semantic information systems [In Russian]. Ontology of designing 2014; 4(14): 78-89.

[10] ***Zagorulko YA, Zagorulko GB***. Ontological approach to development of the decision support system for oil-and-gas production enterprise [In Russian]. NSU Vestnik. Series: "Information Technology" 2012; 10(1): 121-128.

[11] ***Vorozhtsova TN***. Ontology as the basis for the development of intelligent cybersecurity systems [In Russian]. *Ontology of designing*. 2014; 4(14): 69-77.

[12] ***Gaskova D, Massel A***. Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility. Proc. of the 3rd Russian-Pacific Conf. on Computer Technology and Applications (RPC). – Vladivostok. Publisher: IEEE; 2018: 1-5.

[13] ***Massel AG***. The method of threat analysis and risk assessment of violation of information technology security of energy complexes [In Russian]. Proc. of the XX Baikal All-Rus. Conf. "Information and mathematical technologies in science and management". – Irkutsk. MESI SB RAS; 2015; Vol. 3: 186-195.

[14] Industrial companies: attack vectors. Positive Technologies [In Russian]. April 23, 2018. - 24 p. - https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/.

[15] ***Yudin A, Pirogov G.*** Analysis and evaluation of regulatory documents used to ensure information security of Smart Grid systems [In Russian]. Legal, regulatory and metrological support of information security in Ukraine. – Kiev: Igor Sikorsky Kyiv Polytechnic Institute; 2013: 88-95.

[16] ***Litvinov P***. Simulation modeling of information security issues as a tool for security assessment and cost optimization [In Russian]. - http://www.rtsoft.ru/press/23432/imitatsionnoe-modelirovanie-voprosov-informatsionnoy-bezopasnosti-kak-instrument-otsenki-zashchishch/.

[17] ***Mohor VV, Bogdanov AM, Kilevoj AS.*** Information Technology. Methods of security. Cybersecurity manual (ISO/IES 27032:2012) [In Russian]. – Kiev: Three-K; 2013, p.129.

[18] ***Gaskova DA, Massel AG***. Development of expert system for analysis of cybersecurity threats in the energy systems [In Russian]. Information and mathematical technologies in science and management 2016; 1(27): 113-122.

[19] Information security data bank [In Russian]. FAA «GNIII PTZI FSTEK of Russia». - https://bdu.fstec.ru/.

[20] International Vulnerability Database Common Vulnerabilities and Exposures (CVE) - https://cve.mitre.org.

[21] WannaCry in industrial networks: work on the bugs [In Russian]. - https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/.

[22] Positive Research 2018 [In Russian]. Collection of studies on practical security. Positive Technologies JSC. 2018. 204 p. - https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf.

[23] ***Sridhar S, Hanh A, Govindarasu M***. Cyber-physical system security for the electric power grid. Proc. IEEE. 2012; 100(1): 210-224.

[24] ***Massel LV, Pjatkova EV.*** Application of Bayesian belief networks for the intelligent support of energy security problem researches [In Russian]. Proceedings of Irkutsk State Technical University 2012; 2(61): 8-13.

[25] ***Musina VF***. Bayesian belief networks as probabilistic graphical model for economical risk assessment [In Russian]. SPIIRAS Proceedings 2013; 2(25): 235-254.

[26] ***Dantu R, Kolan P***. Risk management using behavior based Bayesian networks. Intelligence and Security Informatics 2005:165-184.

[27] ***Massel AG, Gaskova DA***. Scenario approach for analyzing extreme situations in energy from a cybersecurity perspective. Industry 4.0. – Sofia.Publ.: Scientific Technical Union of Mechanical Engineering "Industry 4.0". 2018; 5: 266-269.

[28] ***Kolosok I, Korkina E***. Cyber Resilience of SCADA at the Level of Energy Facilities. Proc. of the Vth International workshop "Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security" (IWCI 2018). Publ. Atlantis Press. 2018: 100-105.

[29] ***Zio E***. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering and System Safety 2016; 152: 137–150.

[30] ***Machutov NA, Gadenin MM***. Ensuring the safe operation of the technosphere facilities and the public using risk criteria [In Russian]. Conf. abs. of XXI International Scientific and Practical Conference on the problems of protecting the population and territories from emergency situations; 2016: 137-146.

[31] ***Massel LV, Massel AG, Myakotina AY***. Expert system "Advice" for the selection of control actions in situational control in the energy [In Russian]. Proc. of the XX Baikal All-Rus. Conf. "Information and mathematical technologies in science and management" (Russia, Irkutsk. 29 June – 07 July). – Irkutsk. MESI SB RAS; 2015:132-138.

[32] ***Bagrova LA, Bokov VA, Mazinov SA***. Dangerous technological disasters in the energy sector as environmental risk factors [In Russian]. Scientific Notes of Taurida National V.I. Vernadsky University. – Series: Geography Sciences. 2012; 25(2): 9-19.

[33] ***Barabanov AV, Dorofeev AV, Markov AS, Cirlov VL***. Seven secure information technologies [In Russian]. – Moscow. Publ: DMK Press; 2017. – 224 c.

Сведения об авторах

Массель Алексей Геннадьевич, 1985 г. рождения. Окончил Иркутский государственный университет в 2007 г., к.т.н. (2011). Старший научный сотрудник лаборатории информационных технологий в энергетике Института систем энергетики им. Л.А. Мелентьева СО РАН, доцент кафедры «Автоматизированные системы» Института кибернетики Иркутского национального технического университета. В списке научных трудов более 60 работ в области семантического моделирования, проектирования информационных систем и технологий, разработки систем интеллектуальной поддержки принятия решений в области энергетики.

Massel Aleksei Gennadievich (b. 1985) graduated from the Irkutsk State University in 2007, PhD in Engineering Science (2011). Senior researcher of Information Technologies Laboratory in Melentiev Energy Systems Institute SB RAS. Senior lecturer of Automated Systems Department of the Cybernetic Institute in the Irkutsk National Research Technical University. The list of scientific works includes more than 60 articles in the field of semantic modeling, design of information systems and technologies, and the development of intelligent decision support systems in the field of energy solutions.

Гаськова Дарья Александровна, 1993 г. рождения. Окончила Иркутский национальный технический университет в 2015 г. Аспирант лаборатории информационных технологий в энергетике Института систем энергетики им. Л.А. Мелентьева СО РАН. В списке научных трудов более 15 работ в области семантического моделирования, кибербезопасности, менеджмента рисков и разработки интеллектуальных систем.

Gaskova Daria Aleksandrovna (b. 1993) graduated from the Irkutsk National Research Technical University in 2015. Ph.D. student in Information Technologies Laboratory in Melentiev Energy Systems Institute SB RAS. The list of scientific works includes more than 15 articles in the field of semantic modeling, cybersecurity, risk management, and the development of intelligent decision support systems in the field of energy solutions.