ТЕХНОЛОГИЯ АНАЛИЗА КИБЕРУГРОЗ И ОЦЕНКА РИСКОВ НАРУШЕНИЯ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Гаськова Д.А.[1], Массель А.Г.[2]

Энергетическая инфраструктура рассматривается как критическая инфраструктура, представленная топливно-энергетическим комплексом, интегрирующим совокупность энергетических систем, включающих отдельные энергетические объекты. Предлагается методический подход для выявления уязвимостей и угроз информационно-технологических систем энергетических объектов критической инфраструктуры, основанный на применении методов семантического моделирования. Для поддержки методического подхода разрабатывается интеллектуальная система анализа киберугроз и оценки рисков нарушений кибербезопасности.

***Цель:** разработка технологии анализа киберугроз и оценки рисков нарушения кибербезопасности энергетической инфраструктуры с применением предложенного методического подхода и разрабатываемой интеллектуальной системы.*

***Метод:** системный анализ процесса нарушения кибербезопасности на объектах критической инфраструктуры, сопровождающегося реализацией киберугроз, способных вызвать экстремальные ситуации в энергетике.*

***Полученный результат:** предложена новая технология анализа киберугроз и оценки рисков нарушения кибербезопасности критической инфраструктуры, основанная на использовании авторской интеллектуальной системы. Предложенная технология включает этапы выявления киберугроз; моделирования сценариев экстремальных ситуаций, вызванных реализацией киберугроз; оценивания рисков и ранжирования активов информационно-коммуникационной системы энергетического объекта по степени их критичности, и позволяет выполнить оценку количества критически уязвимых активов, обосновать состав и вероятность реализации киберугроз, способных вызвать экстремальные ситуации в энергетике, а также провести оценивание рисков от их реализации на энергетическом объекте. Применение предложенной технологии позволяет автоматизировать процесс анализа киберугроз и оценки рисков нарушения кибербезопасности энергетических объектов.*

***Ключевые слова:** интеллектуальная система, методы семантического моделирования, экстремальные ситуации в энергетике, энергетический сектор, анализ киберугроз, байесовские сети доверия, сценарий угроз.*

DOI: *10.21681/2311-3456-2019-2-42-49*

Введение

Особенность исследования критических инфраструктур заключается в их большой значимости для экономики и населения страны [1], а также сложных и зачастую неявных взаимозависимостях, обширной физической инфраструктуре [2]. Критической инфраструктурой называют часть гражданской инфраструктуры, представляющую собой совокупность физических или виртуальных систем и средств, важных для государства в такой мере, что их выход из строя либо уничтожение может привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации [1]. В исследованиях энергетической безопасности (ЭБ) энергетика России рассматривается как отдельная критическая инфраструктура [3].

В России сейчас активно идет формирование нового института правового регулирования информационной безопасности, направленного на защиту критической информационной инфраструктуры (КИИ) [4]. Риски критической инфраструктуры, относящиеся к категориям запроектных и гипотетических, являются наименее изученными [5]. К данным категориям можно отнести риски последствий на стороне физической инфраструктуры от реализации киберугроз, способных вызывать экстремальные ситуации на объектах энергетики, что становится особенно актуальным при цифровой трансформации энергетики. Нормативно-методическая и правовая базы обеспечения в области кибербезопасности, применимые для энергетического сектора, также находятся в стадии формирования [6]. Несмотря на публикации отчетов об инцидентах в области кибербезопасности крупными компаниями по безопасности [7-9], официальной статистики нет. Ввиду отсутствия статистических данных по киберинцидентам, а также сложности и обширности как информационно-телекоммуникационной, так и физической инфраструктуры объектов энергетического сектора, предлагается использовать семантические методы моделирования для анализа возникновения и развития экстремальных ситуаций в энергетике.

Нештатные ситуации, такие как критические или чрезвычайные, в энергетическом секторе являются предметом исследований энергетической безопасности. Угрозами энергетической безопасности являются дефицит потребностей в ресурсах приемлемого качества

1 Гаськова Дарья Александровна, аспирант, Институт систем энергетики им. Л.А. Мелентьева СО РАН, г. Иркутск, Россия. E-mail: gaskovada@gmail.com.

2 Массель Алексей Геннадьевич, кандидат технических наук, Институт систем энергетики им. Л.А. Мелентьева СО РАН, г. Иркутск, Россия. E-mail: amassel@gmail.com.

в нормальных условиях и экстремальных ситуациях, нарушение стабильности и бесперебойности энергообеспечения [10].

Предложено рассматривать киберугрозы как один из видов стратегических угроз энергетической безопасности [11]. Ситуация осложняется тем, что пока в нашей стране не разработаны методические документы, регламентирующие порядок моделирования угроз для объектов КИИ [12].

Для определения влияния киберугроз на возникновение экстремальных ситуаций авторами предлагаются методический подход и технология анализа киберугроз и оценки рисков нарушения кибербезопасности энергетических объектов, и поддерживающая их интеллектуальная система.

Методический подход к анализу киберугроз и оценке рисков

Методический подход к анализу киберугроз и оценки рисков нарушения кибернетической безопасности критической инфраструктуры на примере энергетики включает три методики:

- методику анализа киберугроз энергетической инфраструктуры;
- методику формирования сценариев экстремальных ситуаций, вызванных реализацией киберугроз, в энергетике;
- методику оценивания рисков нарушения кибербезопасности энергетической инфраструктуры.

Методика анализа киберугроз энергетической инфраструктуры разработана в соответствии со стандартом ISO/МЭК 27005-2011 на основе методики анализа киберугроз и оценки рисков информационно-технологической безопасности энергетических комплексов [13].

В ходе анализа киберугроз решаются следующие задачи:

1) установление контекста;

2) проведение аудита безопасности, включающего:

а) анкетирование;

б) выявление киберуязвимостей в активах информационно-технологической системы (ИТС);

в) оценивание активов ИТС;

г) выявление угроз;

д) выявление типовых векторов атак.

3) формирование концептов сценария.

Анализ киберугроз энергетической инфраструктуры сопровождается инвентаризацией объектов энергетики, установлением значимости активов, которое предлагается осуществлять на основе скорректированных номинальных шкал с учетом индикативного анализа [14], а также категорированием уязвимостей и угроз.

Методика формирования сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз, основывается на системном анализе и исследованиях энергетической безопасности, в частности, на исследованиях развития систем энергетики (СЭ) и топливно-энергетического комплекса (ТЭК) в целом [3]. В качестве инструмента сценарного анализа влияния киберугроз на возникновение экстремальных ситуаций в энергетике предлагается применять байесовские сети доверия (БСД), зарекомендовавшие себя в исследованиях энергетической безопасности ранее [15].

Методика включает 5 основных этапов:

1) формирование концептов сценария и их взаимосвязей;

2) установление вероятностных характеристик, критериев и условий сценария;

3) проведение вычислительного эксперимента и определение вероятности наступления последствий ущербов;

4) построение частной модели угроз;

5) анализ альтернативных сценариев.

В работе частная модель угроз представлена в виде графовой модели, описывающей причинно-следственную цепочку угроз кибернетической и энергетической безопасности, причин их возникновения, последствий, а также вероятность их наступления и степень критичности экстремальной ситуации.

Методика оценивания рисков нарушения кибербезопасности энергетической инфраструктуры направлена на выявление рисков, их качественное и количественное оценивание, а также ранжирование рассмотренных энергетических объектов по установленным критериям, в качестве которых могут выступать величины как интегрального показателя рисков по объекту, так и показатели отдельных типов рисков, связанных с каскадными авариями, экологическими последствиями, безальтернативностью энергоресурсов для потребителей и другое.

Методика содержит рекомендации по описанию риска, качественному и количественному оцениванию, выбору шкал оценивания и ранжирования энергетических объектов.

Методика включает 3 основных этапа:

1) описание рисков;

2) качественное и/или количественное оценивание рисков;

3) ранжирование объектов.

Для поддержки предложенного методического подхода разрабатывается интеллектуальная система анализа киберугроз и оценки рисков нарушения кибербезопасности критической инфраструктуры.

Интеллектуальная система анализа киберугроз и оценки рисков

Интеллектуальная система (ИС) интегрирует три основных блока: 1) экспертную систему для проведения аудита безопасности на предприятии с целью выявления уязвимостей ИТС объекта, определения актуальных угроз, а также формирования перечня значимых активов ИТС; 2) блок Байесовских сетей для формирования сценария и анализа угроз (кибернетической и энергетической безопасности) и последствий от их реализации, в совокупности приводящих к экстремальной ситуации; 3) блок оценивания рисков наступления экстремальной ситуации [16]. Архитектура ИС приведена на рис.1.

В настоящее время реализованы научные прототипы блоков ИС.

Продукционная экспертная система “Cyber” реализована на основе объектно-ориентированного подхода. Модель знаний представляет собой базовую модель

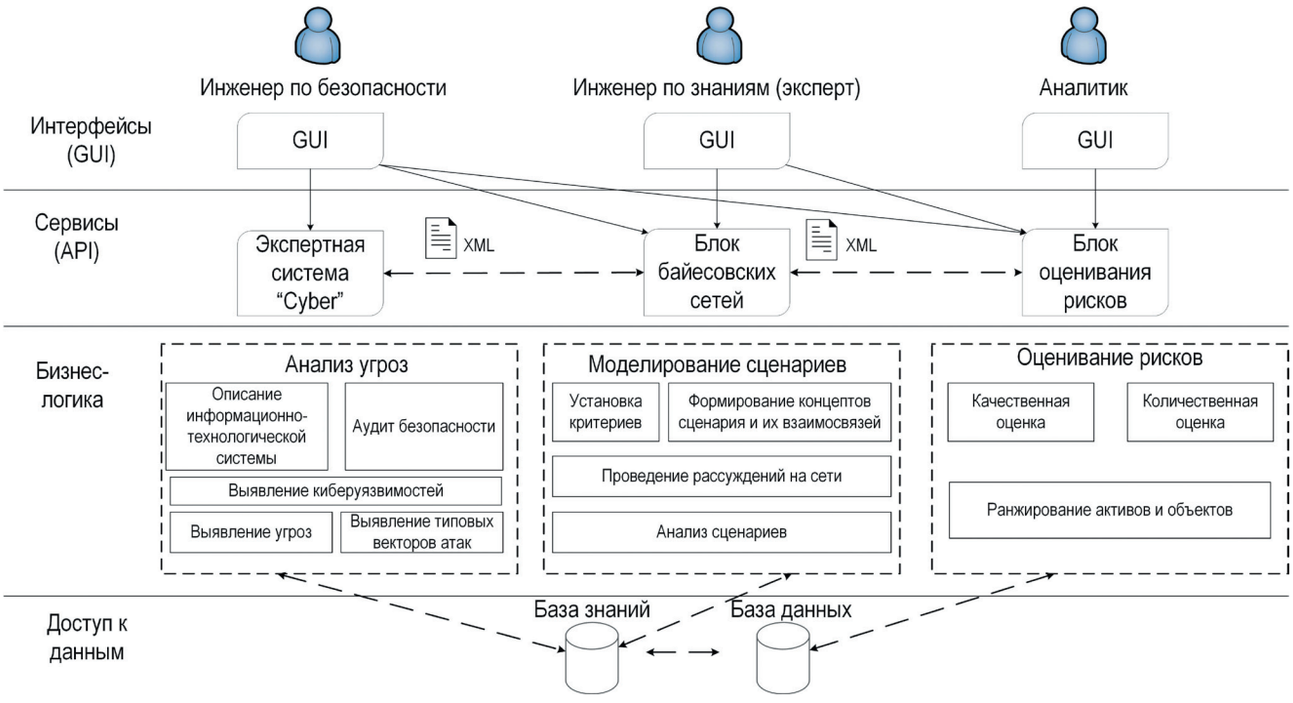

Рис.1. Архитектура интеллектуальной системы

угроз, под которой понимается систематизированный перечень киберугроз информационно-коммуникационной среды и физического оборудования организации, которая также включает классификации объектов ТЭК, активов ИТС, их уязвимостей и их источников.

Блок для формирования сценариев экстремальных ситуаций, вызванных реализацией киберугроз, разрабатывается на основе байесовской сети доверия. На основе БСД пользователем решаются задачи по вероятностному прогнозированию последствий для энергетического объекта от использования уязвимостей нарушителем и реализации угроз кибернетической и энергетической безопасности путем осуществления прямого вывода. Оценки ожидания проявления того или иного состояния в модели основываются на байесовских вероятностях.

Компонент блока качественного оценивания рисков разработан с учетом возможности описания риска, классификации риска по шкале «допустимый», «средний», «критический», а также отображения рисков на тепловой карте и лепестковой диаграмме.

3. Технология анализа киберугроз и оценки рисков нарушения кибербезопасности критических инфраструктур

Для решения задачи анализа киберугроз и оценки рисков нарушения кибербезопасности критической инфраструктуры на примере энергетики разработана технология, которая реализует алгоритм применения предлагаемых методик с использованием разрабатываемой интеллектуальной системы.

Технология состоит из четырех основных этапов:

1) анализ киберугроз:

1.1) установление контекста;

1.2) аудит безопасности;

1.3) формирование концептов сценария;

2) моделирование сценариев:

2.1) декомпозиция угроз;

2.2) формирование сценария;

2.3) установка критериев;

2.4) установка оценок вероятностей значений концептов (переменных);

2.5) провидение рассуждений на сети;

2.6) формирование частной модели угроз;

2.7) анализ сценариев;

3) оценивание рисков;

4) ранжирование объектов.

Предлагаемая технология рассчитана на следующие группы пользователей:

- инженер по безопасности, т.е. специалист в области информационной безопасности предприятия, либо, при отсутствии такового, администратор локальной вычислительной сети;

- инженер по знаниям в энергетике (эксперт): в зависимости от уровня детализации исследования может быть, как экспертом в области энергетической безопасности, так и оператором / инженером-энергетиком на объекте; в области безопасности: инженер по безопасности;

- аналитик, в качестве которого может выступать инженер по знаниям.

Взаимосвязь этапов технологии, методик и блоков интеллектуальной системы представлены в таблице 1.

Дальнейшие действия лиц, принимающих решения по обработке риска, в работе не рассматриваются. В основе технологии лежит цикл Шухарта-Деминга (PDCA). Технология подходит для периодической проверки безопасности, необходимой для проведения в соответствии приказом ФСТЭК от 14 марта

Таблица 1.
Этапы технологии, методики и инструментальные средства

Этапы	Группы пользователей	Методики	Инструментальные средства
Анализ киберугроз	Инженер по безопасности	Методика анализа киберугроз энергетической инфраструктуры	Экспертная система
Моделирование сценариев	Инженер по безопасности; Инженер по знаниям (эксперт в области энергетической безопасности);	Методика формирования сценариев экстремальных ситуаций в энергетике	Блок байесовских сетей доверия
Оценивание рисков	Инженер по знаниям (эксперт); Аналитик;	Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры	Блок оценивания рисков
Ранжирование объектов	Аналитик		

2014 года № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Технология в общем виде в нотации BPNM 2.0 для каждой роли пользователей представлена на рисунке 2.

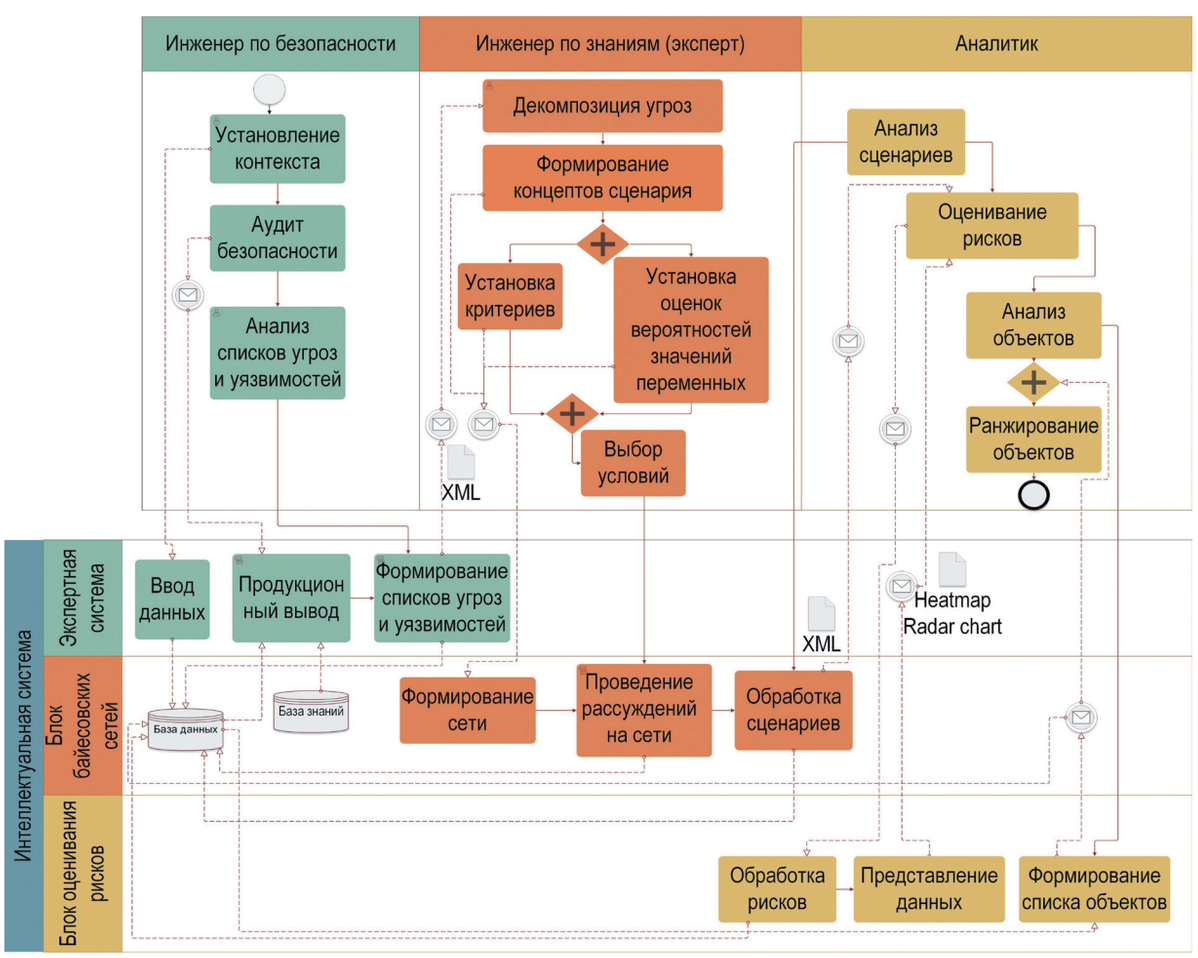

Рис.2. Технология анализа киберугроз и оценки рисков нарушения кибербезопасности критической инфраструктуры в нотации BPMN 2.0

Далее более подробно рассмотрены этапы технологии.

3.1. Этап «Анализ киберугроз»

На данном этапе осуществляется установление контекста т.е. описание основных характеристик рассматриваемого объекта, идентификация и описание активов информационно-технологической системы.

Аудит безопасности энергетического предприятия на начальных этапах состоит в определении критических компонентов и выявлении существующих уязвимостей [13].

Анализ киберугроз в интеллектуальной системе осуществляется с помощью входящей в ее состав продукционной экспертной системы. Формируются перечни критических активов и выявленных уязвимостей, соответствующие им киберугрозы, а также типовые векторы атак, представляющие собой цепочку уязвимостей, угроз и целевых активов. На основе полученного результата формируются концепты и связи между ними для дальнейшего построения сценариев. Формально выходные данные первого этапа технологии анализа киберугроз и оценки рисков представлен формулой (1).

$$P=\{V_i,T_j,A_k,R_a^v\}, \quad (1)$$

где: P – модель атак нарушителя на критические активы, представленная цепочками уязвимостей и угроз; V_i, – выявленные уязвимости информационно-технологической системы энергетического объекта, T_j – угрозы кибербезопасности и энергетической безопасности, A_k – целевые активы атак, R_a^v – векторы атак.

Далее модель угроз передается в виде XML-файла, хранящего переменные, их описание и состояния, а также связи между ними в терминах графовой модели.

3.2. Этап «Моделирование сценариев»

Предлагается сценарное планирование [17] с применением инструмента байесовских сетей доверия. Сценарии оцениваются интегральным показателем вероятности возникновения экстремальной ситуации на энергетическом объекте. Такие ситуации рассматриваются как пессимистический сценарий – набор событий и взаимосвязей между ними, которые приводят к максимальным потерям и ущербу в результате их возникновения и развития [18].

Ранее инструмент байесовских сетей доверия применялся для моделирования рисков возникновения критических ситуаций в энергетике при реализации стратегических угроз ЭБ [15], но угрозы кибербезопасности при этом не рассматривались. Кроме того, БСД применялись при моделировании экономических рисков [19], а также рисков информационных технологий [20].

В связи с включением киберугроз в число стратегических угроз ЭБ [11] предложена следующая структура типового сценария экстремальной ситуации в энергетике, вызванной реализацией киберугроз, описываемая формулой (2):

$$S=\{X^F,X^V,X^T,X^C\}, \quad (2)$$

где: S – структура сценария экстремальной ситуации в энергетике, вызванной реализацией киберугроз; X^F – переменные, соответствующие факторам, влияющим на возникновение экстремальной ситуации; X^V – переменные для обозначения уязвимостей активов ИТС; X^T – переменные для обозначения угроз; X^C – переменные, соответствующие последствиям, связанным с вероятным наступления экстремальной ситуации в энергетике.

Далее выполняется построение сценариев возникновения экстремальных ситуаций при известных условиях состояния ИТС объекта и вероятных угрозах с учетом информации о распространенных векторах атак. На основе анализа сценариев принимаются управленческие решения как порядок действий, необходимых для достижения предпочтительных состояний и ситуаций [21].

3.3. Этап «Оценивание рисков»

Риск рассматривается как сочетание последствий некоторого события (инцидента) и связанной с ним возможности возникновения в соответствии с международным стандартом ISO/IEC 27005:2011 «Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности».

Риски реализации цепочек угроз, приводящих к экстремальной ситуации, оцениваются как качественными, так и количественными методами. Описание таких рисков основывается на качественной информации, полученной от экспертов (специалист в области информационной безопасности, инженер по знаниям в области энергетики), необходимой для определения и описания каждого из шести вышеописанных типов концептов сценария. Количественная информация, связанная с особенностями функционирования системы, используется далее при заполнении значений в концептах.

В работе рассматривается взаимосвязь рисков информационных технологий и рисков аварий и катастроф сложных техногенных систем [4]. Измерение уровня риска осуществляется для всех значимых сценариев, которым присваиваются значения вероятности и последствий риска.

Наличие уязвимости при оценке риска позволяет определить список критических активов на предприятии с целью дальнейшего обоснования финансовых затрат на обеспечение безопасности. Оценивание рисков осуществляется с учетом установленных критериев оценки.

3.4. Этап «Ранжирование объектов»

Этот этап технологии заключается в ранжировании объектов по установленным критериям и уровням риска для каждого из них. С вступлением в силу федерального закона № 187-ФЗ «О защите критической информационной инфраструктуры в Российской Федерации» в каждом секторе экономики должны быть определены критически важные объекты (КВО). Критически важными объектами называют ключевые объекты (или их совокупности) соответствующих инфраструктур, воздействие на которые может оказать наиболее негативный эффект на отрасль экономики, ключевой ресурс или всю инфраструктуру [2].

В рамках предлагаемой технологии ранжирование объектов происходит в соответствии с величиной рисков возникновения экстремальной ситуации, охваты-

вающей некоторую территорию и группу энергетических объектов в их взаимосвязи с другими объектами критических инфраструктур, информация о которых заложена в сценарии в качестве концептов последствий, внешних угроз или факторов. Предложен критерий ранжирования (3):

$K^S=\{C,R,O\}$, (3)

где: K^S – критерий значимости; C – критерий оценки рисков, R – интегральный показатель рисков объекта, O – объект, представленный совокупностью основных характеристик. Итогом этого этапа является проранжированый список объектов.

Заключение

В работе представлены основные положения предлагаемого методического подхода и описание разрабатываемой интеллектуальной системы, объединенных в технологию анализа киберугроз и оценки рисков нарушения кибербезопасности энергетических объектов. В условиях формально не определенного нормативного пространства по обеспечению защиты критических объектов и критической информационной инфраструктуры предлагается технология, направленная на определение объектов энергетики, наиболее подверженных риску нарушения кибербезопасности, определению критических последствий, их вероятности и ущербов, а также формирования ранжированного списка таких объектов.

Предложенная технология в сравнении с традиционными подходами к обеспечению безопасности направлена на определение уязвимостей и киберугроз, реализация которых может вызвать нарушение функционирования энергетического объекта в такой мере, что можно расценивать инцидент как экстремальную ситуацию в энергетике.

Достоверность предложенной технологии на этапе разработки подтверждается экспертными оценками специалистов в области энергетики и кибербезопасности, которые будут подкреплены ее дальнейшей апробацией.

Результаты получены в рамках выполнения проекта по госзаданию ИСЭМ СО РАН №АААА-А17-117030310444-2, отдельные аспекты прорабатывались 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.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент Московского государственного технического университета имени Н.Э. Баумана, Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах // Зарубежное военное обозрение. 2012. № 1. С. 19-30.
2. Массель Л.В. Конвергенция исследований критических инфраструктур, качества жизни и безопасности // Труды VI Международной научной конференции «Информационные технологии и системы». 2017. С. 170-175.
3. Пяткова Н.И., Береснева Н.М. Моделирование критических инфраструктур энергетики с учетом требований энергетической безопасности // Информационные и математические технологии в науке и управлении. 2017. № 3 (7). С. 54-65.
4. Капустина Е.С. Критическая информационная инфраструктура: новые правила и требования к безопасности // Электронный журнал «Финансовые и бухгалтерские консультации». 2018. № 3. С. 4-5.
5. Махутов Н.А., Абросимов Н.В., Гаденин М.М. Обеспечение безопасности – приоритетное направление в области фундаментальных и прикладных исследований // Экономические и социальные перемены: факты, тенденции, прогноз. 2013. № 3 (27). С. 46-71.
6. Васильев В.И, Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 66-74.
7. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018 [Электронный ресурс] // Kaspersky Lab ICS CERT, 27 марта 2019. URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018 (дата обращения к ресурсу: 07.04.2019).
8. Positive Research 2018. Сборник исследований по практической безопасности [Электронный ресурс] // Positive Technologies, 10 июля 2018. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf (дата обращения к ресурсу: 07.04.2019).
9. Отчёт Центра мониторинга за первое полугодие 2018 года [Электронный ресурс] // Перспективный мониторинг, 27 сентября 2018. URL: https://amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2018-1_amonitoring_halfyear_report.pdf (дата обращения к ресурсу: 07.04.2019).
10. Пяткова Н.И., Рабчук В.И., Сендеров С.М., Чельцов М.Б. Энергетическая безопасность России: проблемы и пути решения / Отв. ред. Воропай Н.И. – Новосибирск: Изд-во СО РАН, 2011. – 211 с.
11. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности // Вопросы кибербезопасности. 2016. №4 (17). С. 2-10.
12. Дащенко Ю. Моделирование угроз в условиях методической неопределенности. [Электронный ресурс] // Kaspersky Lab ICS CERT, 11 декабря 2018. URL: // https://ics-cert.kaspersky.ru/media/KL-ICS-CERT-Model-ugroz.pdf (дата обращения к ресурсу: 13.02.2019).
13. Массель А.Г. Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов // Труды XX Байкальской Всероссийской конференции. т. III. – Иркутск: ИСЭМ СО РАН. 2015. С. 186-195.
14. Сендеров С.М., Рабчук В.И. Состояние энергетической безопасности России на федеральном уровне: методический подход к оценке и основные результаты // Известия РАН. Энергетика. 2018. №2. С. 3-12.

15. Массель Л.В., Пяткова Е.В. Применение байесовских сетей доверия для интеллектуальной поддержки исследований проблем энергетической безопасности // Вестник ИрГТУ. 2012. № 2. С. 8-13.
16. Gaskova D., Massel A. Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility [Электронный ресурс] // IEEE Xplore, 8 октября 2018. URL: https://ieeexplore.ieee.org/document/8482229/ (дата обращения к ресурсу: 2.02.2019).
17. Massel A.G., Gaskova D.A. Scenario approach for analyzing extreme situations in energy from a cybersecurity perspective // Industry 4.0. Publisher: Scientific Technical Union of Mechanical Engineering “Industry 4.0”. 2018. № 5. P. 266-269.
18. Кульба В.В., Шульц В.Л., Шелков А.Б Информационное управление. Часть 2: Сценарный подход // Национальная Безопасность / NOTA BENE. 2009. №4. С. 4-15.
19. Мусина В.Ф. Байесовские сети доверия как вероятностная графическая модель для оценки экономических рисков // Труды СПИИРАН. 2013. № 25. С.235-254.
20. Dantu R. Kolan P. Risk management using behavior based Bayesian networks // Intelligence and Security Informatics. 2005. P. 165-184.
21. Феофанов К.А. Сценарные возможности современного прогнозирования и управления // Вестник МГТУ Станкин. 2009. № 4. С. 126-132.

THE TECHNOLOGY OF CYBER THREAT ANALYSIS AND RISK ASSESSMENT OF CYBERSECURITY VIOLATION OF CRITICAL INFRASTRUCTURE

Gaskova D.A.[3], Massel A.G.[4]

The energy infrastructure is considered as a critical infrastructure, represented by energy sector, integrating a set of energy systems that include separate energy facilities. The authors propose the technical approach for identifying vulnerabilities and threats of information and technology systems of energy facilities of critical infrastructure, based on the use of semantic modeling methods. The intelligent system for cyber threat analysis and risk assessment of cybersecurity violation is being developed to support the technical approach.

The purpose: *development of the technology of cyber threat analysis and risk assessment of cybersecurity violation of critical infrastructure using the proposed technical approach and intelligent system being developed.*

Method: *system analysis of cyber security violations at critical infrastructure facilities, involving cyber threats implementation that can cause extreme situations in the energy sector.*

The result: *The new technology of cyber threat analysis and risk assessment of cybersecurity violation of critical infrastructure based on the use of the intelligent system was proposed. The proposed technology includes the steps of 1) identifying cyber threats; 2) modeling scenarios of extreme situations caused by the cyber threats implementation; 3) risk assessment and asset rating of the information and communication system of an energy facility according to their degree of criticality. The technology allows ones to assess the number of critically vulnerable assets, justify the composition and probability of cyber threats that can cause extreme situations in the energy sector, and assess risks from their implementation at an energy facility. The application of the proposed technology allows ones to automate the process of analyzing cyber threats and assessing the risks of cybersecurity violation of energy facilities.*

Keywords: *intelligent system, semantic modeling methods, extreme situations in the energy sector, energy sector, cyber threat analysis, Bayesian Belief Networks, threats scenario*

References

1. Kondratev A. Sovremennye tendentsii v issledovanii kriticheskoi infrastruktury v zarubezhnykh stranakh // Zarubezhnoe voennoe obozrenie. 2012. № 1. S. 19-30.
2. Massel L.V. Konvergentsiia issledovanii kriticheskikh infrastruktur kachestva zhizni i bezopasnosti // Trudy VI Mezhdunarodnoi nauchnoi konferentsii “Informatsionnye tekhnologii i sistemy”. 2017. S. 170-175.
3. Piatkova N.I., Beresneva N.M. Modelirovanie kriticheskikh infrastruktur energetiki s uchetom trebovanii energeticheskoi bezopasnosti // Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2017. № 3 (7). S. 54-65.
4. Kapustina E.S. Kriticheskaia informatsionnaia infrastruktura novye pravila i trebovaniia k bezopasnosti // Elektronnyi zhurnal “Finansovye i bukhgalterskie konsultatsii”. 2018. № 3. S. 4-5.
5. Makhutov N A., Abrosimov N.V., Gadenin M.M. Obespechenie bezopasnosti prioritetnoe napravlenie v oblasti fundamentalnykh i rikladnykh issledovanii // Ekonomicheskie i sotsialnye peremeny: fakty, tendentsii, prognoz. 2013. № 3 (27). S. 46-71.

3 Daria Gaskova, Ph.D. student, Melentiev Energy Systems Institut of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia. E-mail: gaskovada@gmail.com

4 Aleksei Massel, Ph.D., Melentiev Energy Systems Institut of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia. E-mail: amassel@isem.irk.ru

6. Vasilev V.I., Kirillova A.D. Kukharev S.N. Kiberbezopasnost avtomatizirovannykh sistem upravleniia promyshlennykh obieektov sovremennoe sostoianie tendentsii // Vestnik UrFO. Bezopasnost v informatsionnoi sfere. 2018. № 4 (30). S. 66-74.
7. Landshaft ugroz dlia sistem promyshlennoi avtomatizatsii. Vtoroe polugodie 2018 [Elektronnyi resurs] // Kaspersky Lab ICS CERT, 27 marta 2019. URL: https ics-cert kaspersky ru reports 2019 03 27 threat-landscape-for-industrial-automation-systems-h2-2018 (data obrashcheniia k resursu: 07.04.2019).
8. Positive Research 2018. Sbornik issledovanii po prakticheskoi bezopasnosti [Elektronnyi resurs] // Positive Technologies, 10 iiulia 2018. URL: https www ptsecurity com upload corporate ru-ru analytics Positive-Research-2018-rus pdf (data obrashcheniia k resursu: 07.04.2019).
9. Otchet Tsentra monitoringa za pervoe polugodie 2018 goda [Elektronnyi resurs] // Perspektivnyi monitoring, 27 sentiabria 2018. URL: https amonitoring ru service security-operation-center1 mssp quarterly-reports 2018-1_amonitoring_halfyear_report pdf (data obrashcheniia k resursu: 07.04.2019).
10. Piatkova N.I., Rabchuk V.I., Senderov S.M., Cheltsov M.B. Energeticheskaia bezopasnost Rossii: problemy i puti resheniia / Otv. red. Voropai N.I. – Novosibirsk: Izd-vo: SO RAN. 2011. – 211 s.
11. Massel L.V., Voropai N.I., Senderov S.M., Massel A.G. Kiberopasnost kak odna iz strategicheskikh ugroz energeticheskoi bezopasnosti // Voprosy kiberbezopasnosti. 2016. № 4 (17). S. 2-10.
12. Dashchenko U. Modelirovanie ugroz v usloviiakh metodicheskoi neopredelennosti [Elektronnyi resurs] // Kaspersky Lab ICS CERT, 11 dekabria 2018. URL: https ics-cert kaspersky ru media KL-ICS-CERT-Model-ugroz pdf (data obrashcheniia k resursu: 13.02.2019).
13. Massel A.G. Metodika analiza ugroz i otsenki riska narusheniia informatsionno-tekhnologicheskoi bezopasnosti energeticheskikh kompleksov // Trudy XX Baikalskoi Vserossiiskoi konferentsii. t. III. – Irkutsk: ISEM SO RAN. 2015. S. 186-195.
14. Senderov S.M., Rabchuk V.I. Sostoianie energeticheskoi bezopasnosti Rossii na federalnom urovne: metodicheskii podkhod k otsenke i osnovnye rezultaty // Izvestiia RAN. Energetika. 2018. № 2. S. 3-12.
15. Massel L.V., Piatkova E.V. Primenenie baiesovskikh setei doveriia dlia intellektualnoi podderzhki issledovanii problem energeticheskoi bezopasnosti // Vestnik IrGTU. 2012. № 2. S. 8-13.
16. Gaskova D. Massel A. Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility [Elektronnyi resurs] // IEEE Xplore, 8 oktiabria 2018. URL: https ieeexplore ieee org document 8482229 (data obrashcheniia k resursu: 2.02.2019).
17. Massel A.G., Gaskova D.A. Scenario approach for analyzing extreme situations in energy from a cybersecurity perspective // Industry 4.0. Publisher: Scientific Technical Union of Mechanical Engineering “Industry 4.0”. 2018. № 5. P. 266-269.
18. Kulba V.V., Shults V.L., Shelkov A.B. Informatsionnoe upravlenie. Chast 2. Stsenarnyi podkhod // Natsionalnaia Bezopasnost / NOTA BENE. 2009. № 4. S. 4-15.
19. Musina V.F. Baiesovskie seti doveriia kak veroiatnostnaia graficheskaia model dlia otsenki ekonomicheskikh riskov // Trudy SPIIRAN. 2013. № 25. S. 235-254.
20. Dantu R. Kolan P. Risk management using behavior based Bayesian networks // Intelligence and Security Informatics. 2005. P. 165-184.
21. Feofanov K.A. Stsenarnye vozmozhnosti sovremennogo prognozirovaniia i upravleniia // Vestnik MGTU Stankin. 2009. № 4. S. 126-132.