УДК 004.8, 004.822
DOI 10.25205/1818-7900-2021-19-2-17-28

Методики анализа киберситуационной осведомленности об энергетическом объекте

Д. А. Гаськова, А. Г. Массель

Институт систем энергетики им. Л. А. Мелентьева СО РАН
Иркутск, Россия

Аннотация

Предлагается осуществлять анализ киберситуационной осведомленности об энергетическом объекте в три этапа: анализ киберугроз энергетической инфраструктуры; моделирование сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз; оценка рисков нарушения кибербезопасности энергетической инфраструктуры. Представлены три методики, соответствующие каждому этапу. В рамках методического аппарата авторы предлагают применять семантические методы для анализа влияния киберугроз на объекты энергетики с учетом энергетической безопасности, которые показывают свою эффективность в условиях отсутствия или неполноты данных при моделировании поведения систем, которое не поддается формальному описанию или достаточно точному прогнозированию. Представлен подход к анализу киберситуационной осведомленности об энергетических объектах как синтез исследований кибербезопасности и ситуационной осведомленности, отличающийся использованием семантического моделирования.

Ключевые слова

киберситуационная осведомленность, критические ситуации в энергетике, семантические методы моделирования, киберугрозы

Благодарности

Результаты получены в рамках выполнения проекта по госзаданию ИСЭМ СО РАН FWEU-2021-0007 № АААА-А21-121012090007-7, отдельные аспекты прорабатывались в рамках проектов, поддержанных грантами РФФИ № 19-07-00351, № 20-010-00204, Бел_мол_а № 19-57-04003

Для цитирования

Гаськова Д. А., *Массель А. Г.* Методики анализа киберситуационной осведомленности об энергетическом объекте // Вестник НГУ. Серия: Информационные технологии. 2021. Т. 19, № 2. С. 17–28. DOI 10.25205/1818-7900-2021-19-2-17-28

The Method of Cyber Awareness Analysis of an Energy Facility

D. A. Gaskova, A. G. Massel

Melentiev Energy Systems Institute SB RAS
Irkutsk, Russian Federation

Abstract

The article proposes to analyze cyber-situational awareness of an energy facility in three stages. There are i) analysis of cyber threats to the energy infrastructure; ii) modeling of extreme situations scenarios in the energy sector caused by the implementation of the cyber threats; iii) risk assessment of the cybersecurity disruption to energy infrastructure. Three methods are presented, corresponding to each stage. The authors propose to apply semantic modeling methods to analyze the impact of cyber threats to energy facilities, taking into account energy security within the presented approach. Such methods show their effectiveness in the absence or incompleteness of data for modeling the behavior of systems, which defies formal description or accurate forecasting. The presented approach to the cyber situational awareness analysis of energy facilities considered as a synthesis of cybersecurity and situational awareness studies, characterized by the use of semantic modeling methods.

Keywords

cyber situational awareness, extreme situations in the energy sector, semantic modeling methods, cyber threats

Acknowledgements

This work was executed within the framework of project on state task MESI SB RAS FWEU-2021-0007 no. AAAA-A21-121012090007-7. The studying of separated aspects was supported by RFBR grants no. 19-07-00351, no. 20-010-00204, no. 19-57-04003

For citation

Gaskova D. A., Massel A. G. The Method of Cyber Awareness Analysis of an Energy Facility. *Vestnik NSU. Series: Information Technologies*, 2021, vol. 19, no. 2, p. 17–28. (in Russ.) DOI 10.25205/1818-7900-2021-19-2-17-28

Введение

Актуальность исследований киберситуационной осведомленности в энергетическом секторе обусловлена, с одной стороны, активно развивающейся тенденцией цифровой трансформации энергетики, а с другой – неполнотой информации об инцидентах, вызванных киберугрозами и разрозненностью руководящих документов в рассматриваемой области, что, в свою очередь, повышает риски внедрения новых информационных технологий в энергетике. Исследования развития энергетического сектора связаны с цифровой трансформацией энергетики, сопровождающейся разработкой и внедрением цифровых технологий, в состав которых включают промышленный Интернет вещей, 3D-моделирование, моделирование и прогнозирование на основе анализа «больших данных» (Big Data), нейросети, облачные и туманные вычисления, виртуальную и дополненную реальность, машинное обучение, компьютерную имитацию на основе цифровых двойников, интеллектуальные датчики, роботизацию производства, аддитивные технологии [1]. Перспективными технологиями в данной области также называют онтологические модели деятельности и распределенные реестры (Blockchain) [2] [1]. Современные решения для автоматизации технологического процесса на энергетических объектах становятся все более сложными и используют передовые цифровые технологии [2], что приводит к увеличению рисков нарушения безопасности этих объектов, вплоть до возникновения экстремальных ситуаций (ЭкС).

Активное развитие и внедрение интеллектуальных технологий на предприятиях послужило предпосылкой появления такого направления исследований, как киберситуационная осведомленность (КСО). Киберситуационная осведомленность (Cyber Situational Awareness) – область исследований, связанная с применением методов искусственного интеллекта в кибербезопасности, направленная на повышение осведомленности о возможных ситуациях нарушений кибербезопасности и автоматическое обнаружение киберугроз [3]. Под термином «киберситуационная осведомленность энергетических объектов» будем понимать осведомленность о состоянии киберсреды энергетических объектов, включающую информацию: о критических уязвимостях энергетических объектов с точки зрения кибербезопасности; о киберугрозах, инициирующих эти критические уязвимости, а также о техногенных угрозах энергетической безопасности, вызванных киберугрозами.

Методики анализа киберситуационной осведомленности об энергетических объектах

Анализ киберситуационной осведомленности об энергетических объектах в нотации IDEF0, отображающей структуру и функции анализа, а также потоки информации и материальных объектов, преобразуемые этими функциями, представлен на рис. 1. Для анализа киберситуационной

[1] Энергетическая Стратегия Российской Федерации на период до 2035 года: распоряжение Правительства Российской Федерации от 9 июня 2020 года № 1523-р // «Собрание законодательства РФ». 15.06.2020. № 24, ст. 3847.

[2] Концепция «Цифровая трансформация 2030» компании «РОССЕТИ», 2018 год. URL: https://www.rosseti.ru/investment/Kontseptsiya_Tsifrovaya_transformatsiya_2030.pdf.

Рис. 1. Контекстная диаграмма анализа киберситуационной осведомленности об энергетических объектах в нотации IDEF0

Fig. 1. Context diagram of the cyber situational awareness analysis of energy facilities in IDEF0 notation

Рис. 2. Декомпозиция первого уровня анализа киберситуационной осведомленности об энергетических объектах в нотации IDEF0

Fig. 2. First level decomposition diagram of the cyber situational awareness analysis of energy facilities in IDEF0 notation

осведомленности об энергетических объектах предложены методики, построены модели структурирования знаний, а именно фрактальная структурированная модель (ФС-модель) [4] и система онтологий [5], выделены источники информации и предложены инструментальные программные средства поддержки этого анализа.

Предлагаемые методики разработаны в соответствии со стандартом ИСО/МЭК 27005-2010 на основе методик анализа угроз и оценки рисков информационно-технологической безопасности энергетических комплексов [6] и моделирования угроз энергетической безопасности с помощью байесовских сетей доверия (БСД) [7].

Основные этапы анализа киберугроз и оценки рисков нарушения кибербезопасности энергетической инфраструктуры представлены на рис. 2. На первом уровне декомпозиции анализа киберситуационной осведомленности энергетических объектов выделены три основных процесса, представленные блоками на диаграмме. Анализ киберугроз энергетической инфраструктуры предлагается выполнять по соответствующей методике с использованием предложенной экспертной системы и дополнительных инструментальных средств, обычно применяемых при проведении аудита безопасности критической информационной инфраструктуры (КИИ). Моделирование сценариев ЭкС в энергетике, вызванных реализацией киберугроз, предлагается выполнять по соответствующей методике с использованием компонента БСД и инструментальных средств, реализующих математическое моделирование энергетических объектов. Оценку рисков предлагается осуществлять с учетом предыдущих процессов, используя компонент оценки рисков. Предлагаемые методики подробно рассмотрены далее.

Методика анализа киберугроз энергетической инфраструктуры включает три этапа.

1. *Описание энергетического объекта и определение критериев оценки* включают описание основных характеристик энергетического объекта (ЭО), бизнес-процессов и КИИ ЭО, в рамках которых определяются системы, их основные компоненты и функциональное назначение, в дальнейшем используемые при формировании предположений о возможных киберфизических последствиях реализации угроз [8]. Для каждого компонента системы определяется состав основных активов (аппаратно-программные, программные, протоколы и пр.). Предлагается в качестве основных критериев оценки угроз и уязвимостей определять критерий значимости (критичности) актива и критерий оценивания уязвимостей и угроз в соответствии со шкалами оценки. Результатом этапа является список активов и их качественная оценка по установленным критериям оценивания.

Для обеспечения приемлемого уровня КСО показатели безопасности должны быть приведены в соответствие с отраслевыми стандартами управления безопасностью компьютеров и сетей, а также с общими организационными и бизнес-целями в корпоративных средах [9] и технологических сегментах локальной вычислительной сети (ЛВС). В работе [9] выделяют 14 метрик безопасности корпоративной сети, где для каждой метрики определены шкала параметров и метод вычисления. В работе [10] представлен метод оценки рисков кибербезопасности на основе теории нечетких множеств, включающий семантические описания шкал выделенных факторов риска.

2. *Анализ уязвимостей и угроз КИИ объекта* включает анализ КИИ с последующим оцениванием активов КИИ, выявлением критически важных активов, выявлением киберуязвимостей в активах КИИ и киберугроз, выделение возможных целевых активов кибератаки. Результатом этапа является список уязвимостей для каждого значимого актива КИИ рассматриваемого объекта и киберугроз, которые могут эти уязвимости реализовать.

3. *Построение модели сценариев ЭкС в энергетике, вызванных киберугрозами*, в виде правил «ЕСЛИ-ТО», которые описывают возможные способы нарушения кибербезопасности энергетического объекта. Включает описание реализации киберугрозы, выделение векторов проникновения и векторов атак на целевые активы, а также их анализ. При этом векторы атак направлены на целевые активы, являющиеся составляющей технологической инфраструктуры энергетического объекта. Результатом этапа являются сценарии (вида цепочки правил

«ЕСЛИ-ТО») реализации всех уязвимостей, представленные цепочками уязвимостей и угроз, приводящих к нарушению нормального функционирования технологической инфраструктуры ЭО и некоторым негативным последствиям.

Методика моделирования сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз, включает четыре этапа.

1. *Формирование узлов и их взаимосвязей в графе БСД-модели* включает построение графа, состоящего из вершин нескольких типов, в соответствии с разработанной структурой сценария (рис. 3), и взаимосвязей между ними на основе построенных ранее правил вида «ЕСЛИ-ТО» (см. далее, формула (1)).

Структура сценария ЭкС в энергетике, вызванных реализацией киберугроз, разработана в соответствии с моделью [11], представлена на рис. 3 и включает следующие типы концептов:

- **уязвимости** (V) – множество всех обнаруженных критических уязвимостей рассматриваемой ЛВС;
- **киберугрозы** (T) – множество киберугроз активов ЛВС;
- **техногенные угрозы** (W) – множество техногенных угроз энергетической безопасности (ЭБ), вызванных киберугрозами T;
- **последствия** (C) – множество последствий реализации угроз T и W.

Структура сценария также включает классификацию концептов по типам, представленным выше, и по сегментам рассматриваемой ЛВС: гостевым, корпоративным, демилитаризованным зонам, технологическим сегментам.

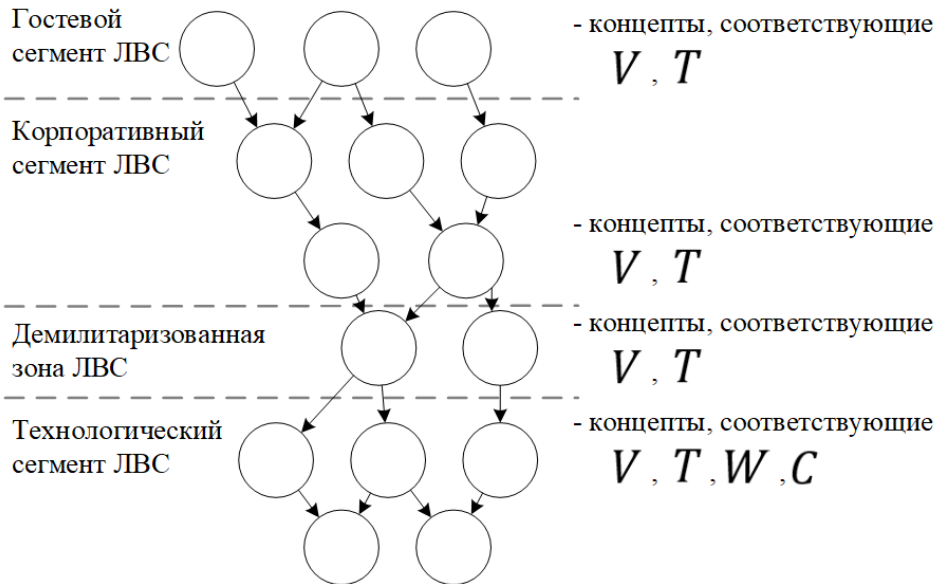

Рис. 3. Визуальное отображение структуры сценария ЭкС в энергетике, вызванных киберугрозами

Fig. 3. Visual display of the scenario structure of extreme situations in the energy sector caused by cyber threats

Такая структура способствует визуальному отображению возможных атак на технологический сегмент ЛВС из различных сегментов ЛВС. Например, в исследовании «Промышлен-

ные компании: векторы атак» [3] приводится типовая схема атаки на технологический сегмент, а в [12] описана модель атаки по этапам.

Графом БСД-модели будем называть ациклический, ориентированный, взвешенный граф G такой, что

$$G = (N, U; q), \tag{1}$$

где N – множество вершин графа, U – множество дуг графа, q – функция на вершинах.

Функция q на вершинах графа G задается как

$$q: N \to B, \tag{2}$$

где B_i – матрица весов вершины N_i. Для каждой вершины N_i элементами этой матрицы являются вероятности соответствующей случайной величины X_i.

2. *Определение вероятностных характеристик сценария* включает заполнение матриц весов для каждой вершины N_i (таблиц условных вероятностей (ТУВ)), на основе опыта эксперта или имеющейся накопленной информации о подобных инцидентах и формирование графа.

Каждой вершине N_i графа G соответствует единственная случайная величина X_i, такая, что

$$X_i \in \{X^V \cup X^T \cup X^W \cup X^C\}, \tag{3}$$

где $i = \overline{1,n}$ и $n = |V| + |T| + |W| + |C|$, X^V – множество случайных величин, соответствующих V, X^T – множество случайных величин, соответствующих T, X^W – множество случайных величин, соответствующих W, X^C – множество случайных величин, соответствующих C. Безусловные вероятности случайной величины X_i задаются в ТУВ в случае, когда у соответствующей вершины N_i предков нет (табл. 1). В случае, когда есть набор предков $pa(X_i)$ вершины N_i, задаются условные вероятности (табл. 2).

Формирование графа G сопровождается заполнением матриц весов B_i для вершин N_i, в данном случае $i = \overline{1,|N|}$. При этом совместное распределение вероятностей на множестве вершин, соответствующих X графа G, называют

$$\begin{gathered} P(X) = (P_1(X), P_2(X), \dots, P_n(X)), \\ P_i(X) = P(X_i | pa(X_i)), \end{gathered} \tag{4}$$

где X_i введено ранее в (3), $pa(X_i)$ – множество предков вершины, соответствующей X_i, в данном случае $n = |N|$.

Таблица 1

Общий вид ТУВ для отображения безусловных вероятностей случайной величины X_i

Table 1

General view of the table of conditional probabilities for displaying the unconditional probabilities of a random variable

X_i.	$\overline{X_i}$
T	F
p	$1-p$

[3] Промышленные компании: векторы атак / Positive Technologies, 2018. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018.

Таблица 2

Общий вид ТУВ для отображения условных вероятностей случайной величины X_i

Table 2

General view of the table of conditional probabilities for displaying the conditional probabilities of a random variable

$pa(X_i)_1$	...	$pa(X_i)_k$	$X_i.$	$\overline{X_i}$
T	T	T	p_1	$1-p_1$
...	...	...	...	...
T	T	T	...	...
F	F	F	...	...
...	...	...	...	...
F	F	F	p_{2^k}	$1-p_{2^k}$

В таблице приняты следующие обозначения: p – вероятность случайной величины X_i, $k = |pa(X_i)|$, T (true) – состояние реализации уязвимости, угрозы или последствия, F (false) – противоположное T состояние.

3. *Проведение вероятностного эксперимента* включает вычисление распределения вероятностей в БСД в зависимости от наблюдаемых уязвимостей и угроз в построенных векторах атак. Проведение расчетов выполняется с целью ответа на вопрос «Как изменится вероятность последствий, если принять, что некоторое множество уязвимостей и / или угроз реализовано?». Такое множество будем называть множеством свидетельств, каждое из которых можно описать утверждением вида «Определенные уязвимости из V и / или угрозы из T, W реализованы». При наличии такого множества свидетельств необходимо пересчитать вероятности дискретных случайных величин X, соответствующих вершинам N графа G.

Вершины, в которые введены свидетельства, имеют множество вершин-потомков. Для того чтобы в каждой из таких вершин-потомков пересчитать апостериорную вероятность (после наблюдения), в их матрицах весов B требуется не учитывать все несовместимые со свидетельством в вершине-предке случаи. Если случай становится невозможным, то его вероятность принимается равной нулю (невозможное событие). Вероятности прочих случаев пересчитываются (блок 2) по формуле Байеса:

$$P(X_i|e) = \frac{\sum_{j=1}^{m} P_j(X,e)}{P(e)}, \quad (5)$$

где $P(X_i|e)$ – апостериорная вероятность X_i, E – множество дискретных случайных величин, являющихся свидетельствами, e – значения этих случайных величин, m – количество оставшихся случайных переменных, в которые не введены свидетельства.

4. *Анализ альтернативных сценариев* включает анализ наиболее уязвимых мест, критических угроз и векторов атак.

Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры включает четыре основных этапа.

1. *Описание рисков* включает списки наблюдаемых уязвимостей и угроз, а также вероятность последствия:

$$R = \{T, V, W, C, D\}, \quad (6)$$

где значения T, V, W, C введены ранее, D – множество ущербов последствий сценариев.

2. *Оценивание рисков* включает расчет и дальнейшее качественное и количественное оценивание. Количественную оценку рисков предлагается выполнять в отношении последствия сценария S_i по формуле

$$R_i = P(c_i) \times D_i, \quad (7)$$

где $P(c_i)$ – вероятность последствия сценария S_i, рассчитываемая по формуле (5), D_i – ущерб от реализации киберугроз этого сценария, $i = \overline{1, 2^n - 1}$.

Принимается, что существует взаимно-однозначное соответствие между сценарием S_i и вероятностью его последствия $P(c_i), i = \overline{1, 2^n - 1}, n = |V| + |T| + |W|$. Условия оценки сценариев ЭкС, вызванных киберугрозами, имеют вид, представленный в табл. 3.

Таблица 3

Условия оценки сценариев ЭкС в энергетике, вызванных киберугрозами

Table 3

Conditions for assessing extreme situations in energy sector scenarios caused by cyber threats

Незначительный уровень опасности	Средний уровень опасности	Высокий уровень опасности
$\begin{cases} 0 \le P(\mathrm{c}_i) \times D_i < l_1 \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (8)	$\begin{cases} l_1 \le P(\mathrm{c}_i) \times D_i < l_2 \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (9)	$\begin{cases} l_2 \le P(\mathrm{c}_i) \times D_i \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (10)

В таблице приняты следующие обозначения: l_1, l_2 – критерии кластеризации сценариев ЭкС, вызванных киберугрозами, D^{m} – максимальный ущерб, $i = \overline{1, 2^n - 1}$.

Все сценарии разбиваются на три кластера: норма, предкризис, кризис:

$$K_s = \{S_{s1}, S_{s2}, \dots, S_{sl}\}, \quad (11)$$

где K_s – множество кластеризованных сценариев ЭкС в энергетике, вызванных киберугрозами, $s = \overline{1,3}$.

3. *Ранжирование активов КИИ и выработка рекомендаций* включает составление списка активов по критерию значимости, по уровню рисков и выработку соответствующих мер по их снижению.

4. *Определение уровня киберситуационной осведомленности* энергетического объекта включает подсчет отношения количества рассмотренных сценариев к количеству возможных сценариев в модели по формуле

$$L = \frac{\gamma}{2^n - 1}, \quad (12)$$

где L – уровень КСО энергетического объекта, γ – количество рассчитанных сценариев, $2^n - 1$ – общее количество сценариев, $n = |V| + |T| + |W|$.

Заключение

В статье предложена методика анализа киберситуационной осведомленности об энергетическом объекте, основанная на вероятностной модели сценариев ЭкС в энергетике, вызванных реализацией киберугроз. Модель, построенная на основе аппарата байесовских сетей доверия, включает в себя структуру сценариев. Описана структура сценария: типы концептов и их распределение по сегментам ЛВС. Предложена метрика оценки КСО, основанная на формировании векторов атак на рассматриваемую ЛВС и байесовском рассуждении на сети.

Список литературы

1. **Zhang C.**, **Romagnoli A.**, **Zhou L.**, **Kraft M.** From Numerical Model to Computational Intelligence: The Digital Transition of Urban Energy System. *Energy Procedia*, 2017, vol. 143, p. 884–890. DOI 10.1016/j.egypro.2017.12.778
2. **Irmak E.**, **Erkek I.** An overview of cyber-attack vectors on SCADA systems. In: 6th International Symposium on Digital Forensic and Security (ISDFS). March, 2018. DOI 10.1109/isdfs.2018.8355379
3. **Frank U.**, **Brynielsson J.** Cyber Situational Awareness – A systematic review of literature. *Computer Security*, 2014, vol. 46, p. 18–31. DOI 10.1016/j.cose.2014.06.008
4. **Gaskova D.** Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security. In: Proceedings of the VI International Workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security (IWCI 2019)". Irkutsk, Atlantis Press, 2019, p. 179–183. DOI 10.2991/iwci-19.2019.31
5. **Гаськова Д. А.**, **Массель А. Г.** Онтологический инжиниринг анализа угроз кибербезопасности критических инфраструктур // Онтология проектирования. 2019. Т. 9, № 2 (32). С. 225–238. DOI 10.18287/2223-9537-2019-9-2-225-238
6. **Массель Л.В.**, **Пяткова Е.В.** Применение байесовских сетей доверия для интеллектуальной поддержки исследований проблем энергетической безопасности // Вестник ИрГТУ. 2012. № 2. С. 8–13.
7. **Массель А. Г.** Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов // Тр. XX Байкальской Всерос. конф. Иркутск: ИСЭМ СО РАН, 2015. Т. 3. С. 186–195.
8. **Дащенко Ю**. Моделирование угроз в условиях методической неопределенности / Kaspersky Lab ICS CERT. URL: https://ics-cert.kaspersky.ru/media/KL-ICS-CERT-Model-ugroz.pdf.
9. **Cheng Y.**, **Deng J.**, **Li J.**, **DeLoach S. A.**, **Singhal A.**, **Ou X.** Metrics of Security. In: Kott A., Wang C., Erbacher R. (eds.). Cyber Defense and Situational Awareness. Advances in Information Security, 2014, vol. 62. Springer, Cham. DOI 10.1007/978-3-319-11391-3_13
10. **Колосок И. Н.**, **Гурина Л. А.** Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы // Информационные и математические технологии в науке и управлении. 2019. № 2 (14). С. 40–51. DOI 10.25729/2413-0133-2019-2-04
11. **Гаськова Д. А.** Метод определения уровня киберситуационной осведомленности энергетических объектов // Информационные и математические технологии в науке и управлении. 2020. № 4 (20). С. 64–74. DOI 10.38028/ESI.2020.20.4.006
12. **Assante M. J.**, **Lee R. M.** The Industrial Control System Cyber Kill Chain. URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-systemcyber-kill-chain-36297.

References

1. **Zhang C.**, **Romagnoli A.**, **Zhou L.**, **Kraft M.** From Numerical Model to Computational Intelligence: The Digital Transition of Urban Energy System. *Energy Procedia*, 2017, vol. 143, p. 884–890. DOI 10.1016/j.egypro.2017.12.778
2. **Irmak E.**, **Erkek I.** An overview of cyber-attack vectors on SCADA systems. In: 6th International Symposium on Digital Forensic and Security (ISDFS). March, 2018. DOI 10.1109/isdfs.2018.8355379
3. **Frank U.**, **Brynielsson J.** Cyber Situational Awareness – A systematic review of literature. *Computer Security*, 2014, vol. 46, p. 18–31. DOI 10.1016/j.cose.2014.06.008

4. **Gaskova D.** Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security. In: Proceedings of the VI International Workshop “Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security (IWCI 2019)”. Irkutsk, Atlantis Press, 2019, p. 179–183. DOI 10.2991/iwci-19.2019.31
5. **Gaskova D. A.**, **Massel A. G.** Ontological engineering for the development of the intelligent system for threats analysis and risk assessment of cybersecurity in energy facilities. *Ontology of designing*, 2019, vol. 9 (2), p. 225–238. (in Russ.) DOI 10.18287/2223-9537-2019-9-2-225-238
6. **Massel L. V.**, **Pyatkova E. V.** Application of Bayesian Networks to Intelligently Support Energy Security Research. *Proceedings of Irkutsk State Technical University*, 2012, no. 2, p. 8–13. (in Russ.)
7. **Massel A. G.** Methods of the analysis of threats, risk assessment violations of information and technological security of energy complexes. In: Proceedings of the XX Baikal All-Russian Conference “Information and mathematical technologies in science and management”. Irkutsk, MESI SB RAS, 2015, vol. 3, p. 186–195. (in Russ.)
8. **Dashchenko Yu.** Threat modeling in conditions of methodological uncertainty. Kaspersky Lab ICS CERT. URL: https://ics-cert.kaspersky.ru/media/KL-ICS-CERT-Model-ugroz.pdf (in Russ.)
9. **Cheng Y.**, **Deng J.**, **Li J.**, **DeLoach S. A.**, **Singhal A.**, **Ou X.** Metrics of Security. In: Kott A., Wang C., Erbacher R. (eds.). Cyber Defense and Situational Awareness. Advances in Information Security, 2014, vol. 62. Springer, Cham. DOI 10.1007/978-3-319-11391-3_13
10. **Kolosok I. N.**, **Gurina L. A.** Cybersecurity Risk Assessment of Information and Communication Infrastructure of Intelligent Energy System. *Information and mathematical technologies in science and management*, 2019, no. 2 (14), p. 40–51. (in Russ.) DOI 10.25729/2413-0133-2019-2-04
11. **Gaskova D. A.** Method for Determining the Level of Cyber Situational Awarenes on Energy Facilities. *Information and mathematical technologies in science and management*, 2020, no. 4 (20), p. 64–74. (in Russ.) DOI 10.38028/ESI.2020.20.4.006
12. **Assante M. J.**, **Lee R. M.** The Industrial Control System Cyber Kill Chain. URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-systemcyber-kill-chain-36297.

Материал поступил в редколлегию
Received
11.02.2021

Сведения об авторах

Гаськова Дарья Александровна, младший научный сотрудник отдела систем искусственного интеллекта в энергетике Федерального государственного бюджетного учреждения науки Институт систем энергетики им. Л. А. Мелентьева Сибирского отделения Российской академии наук (Иркутск, Россия)

gaskovada@gmail.com

Массель Алексей Геннадьевич, кандидат технических наук, старший научный сотрудник отдела систем искусственного интеллекта в энергетике Федерального государственного бюджетного учреждения науки Институт систем энергетики им. Л. А. Мелентьева Сибирского отделения Российской академии наук (Иркутск, Россия)

amassel@gmail.com

Information about the Authors

Daria A. Gaskova, Junior Fellow of Department of Artificial Intelligence Systems in the Energy Sector, Melentiev Energy Systems Institute Siberian Branch of the Russian Academy of Sciences (Irkutsk, Russian Federation)

gaskovada@gmail.com

Aleksei G. Massel, PhD in Engineering Science, Senior researcher of Department of Artificial Intelligence Systems in the Energy Sector, Melentiev Energy Systems Institute Siberian Branch of the Russian Academy of Sciences (Irkutsk, Russian Federation)

amassel@gmail.com