УДК 04.89:519.226.3

МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ КИБЕРСИТУАЦИОННОЙ ОСВЕДОМЛЕННОСТИ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Гаськова Дарья Александровна
м.н.с., e-mail: gaskovada@gmail.com,
Институт систем энергетики им. Л.А. Мелентьева СО РАН,
664033, Россия, г. Иркутск, ул. Лермонтова, 130.

Аннотация. В статье рассматриваются результаты исследования ситуационной осведомленности в киберсреде энергетических объектов. Для повышения информированности о состоянии киберсреды таких объектов предлагаются модель сценариев экстремальных ситуаций в энергетике на основе байесовской сети доверия и численный метод определения киберситуационной осведомленности. Модель основана на причинно-следственных связях между уязвимостями локальной вычислительной сети (ЛВС) и возможных киберугрозах, представленных в виде векторов проникновения в ЛВС, векторов развития кибернетических атак и векторов атак на целевой актив, объединённых в сценарии. В работе ставится акцент на сценарии, последствия которых могут расцениваться как экстремальные ситуации в энергетике, вызванные киберугрозами.

Ключевые слова: байесовские сети доверия, экстремальные ситуации в энергетике, киберугрозы.

Цитирование: Гаськова Д.А. Метод определения уровня киберситуационной осведомлённости энергетических объектов //Информационные и математические технологии в науке и управлении. 2020. № 4 (20). С. 64-74. DOI: 10.38028/ESI.2020.20.4.006

Введение. Исследования кибербезопасности и киберситуационной осведомленности (КСО) в энергетике связаны с исследованиями критических инфраструктур (КИ). Это обусловлено рассмотрением энергетического сектора как одной из основных КИ и защитой ключевых информационных систем объектов КИ как направления кибербезопасности [16]. Нарушение функционирования или разрушение объектов энергетики приводит к экстремальным ситуациям (ЭкС), губительным последствиям и нарушению энергетической безопасности (ЭБ) как составляющей национальной безопасности (НБ) страны, а киберугрозы выделены как группа стратегических угроз в энергетике [4]. В Доктрине энергетической безопасности Российской Федерации [7], принятой в 2019 году, отражены официальные взгляды на обеспечение ЭБ в рамках стратегического планирования в сфере обеспечения НБ. Наряду с такими трансграничными угрозами ЭБ, как террористическая и диверсионная деятельность, неблагоприятные и опасные природные явления, выделены и угрозы противоправного использования информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, способные привести к нарушениям функционирования инфраструктуры объектов топливно-энергетического комплекса (ТЭК). С практической точки зрения наблюдается долгосрочная тенденция реализации кибератак на объектах энергетического сектора. В исследованиях [3] в 2020 году отмечаются достаточно выраженные различия в ландшафте угроз для всех рассматриваемых компьютеров автоматизированной системы управления

(АСУ) и компьютеров АСУ в энергетике в пользу вторых по основным типам угроз, заблокированных на компьютерах, в том числе: интернет-угрозам, почтовым угрозам, угрозам на съемных носителях. В исследованиях атак на ТЭК России [1] за 2018-2019 годы показано, что основными целями киберпреступников, атакующих ТЭК, являются разрушительное воздействие на инфраструктуру и промышленный шпионаж.

Киберситуационная осведомленность. Активно вопросами ситуационной осведомленности начали заниматься ещё в 80-х годах прошлого столетия. Термин «ситуационная осведомленность», или Situational Awareness, тесно связано в первую очередь с пионерными работами Мики Эндсли (Mica R. Endsley) [5, 11], в которых ситуационная осведомленность определена как «чувственное восприятие элементов обстановки в (едином) пространственно-временном континууме, осознанное восприятие их значения, а также проецирование их в ближайшее будущее». В своей работе [12] М. Эндсли отмечала, что проблемы нового класса технологий, заключающиеся в том числе в росте сложности систем и генерации в них огромного объема данных, являются одним из факторов роста интереса к ситуационной осведомленности. Развитие новых информационно-коммуникационных технологий добавило измерение «Cyber» к традиционным военным и деловым операциям ситуационной осведомленности, поскольку системы и сети, работающие в киберпространстве, имеют уязвимости, которые представляют значительные риски как для отдельных организаций, так и для национальной безопасности [17]. Такое измерение и называют киберситуационной осведомленностью.

Определение термина «ситуационная осведомленность» в контексте киберсреды приведено в глоссарии Национального института стандартов и технологий США (NIST) [18], в соответствии с которым ситуационная осведомленность – восприятие мер (стратегий, средств) обеспечения безопасности предприятия и его ландшафта угроз в единой пространственно-временной системе координат; понимание двух этих аспектов вместе (риск); прогноз их состояния на ближайшее будущее *(перевод автора)*.

На основе определений, приведенных в [9, 13, 20,], в контексте этих исследований под киберситуационной осведомленностью понимается область исследований, связанная с применением методов искусственного интеллекта в области кибербезопасности, направленная на повышение осведомленности о возможных ситуациях нарушений кибербезопасности и автоматическое обнаружение киберугроз.

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; киберугрозах, инициирующих эти критические уязвимости, а также о техногенных угрозах энергетической безопасности, вызванных киберугрозами.

Эта сравнительно новая концепция для нашей страны уже получила достаточно широкое распространение за рубежом [9, 10, 13, 19, 20]. Отмечается, что киберситуационная осведомленность не может рассматриваться изолированно, она взаимозависима и является частью ситуационной осведомленности, которая ограничена рамками киберсреды. Киберсреда включает подключенные компьютерные устройства, персонал, инфраструктуру, приложения, сервисы, телекоммуникационные системы, а также совокупность передаваемой и/или хранящейся информации [21]. Самостоятельное понимание ситуационной осведомленности, полученное на основе анализа и оценки действий в сети, рассматривается

как дополнительная информация и знания для получения общей ситуационной осведомленности путем их объединения с информацией и знаниями о параметрах, состояниях, характеристиках системы вне киберсреды [13].

Современные решения для автоматизации технологического процесса на энергетических объектах становятся более сложными и используют передовые цифровые технологии [15], что приводит к увеличению рисков нарушения безопасности этих объектов, вплоть до возникновения экстремальных ситуаций. Ведущим направлением решения проблем обеспечения безопасности являются теории, основанные на концепции риска. Технические системы почти всегда проектируются, конструируются и эксплуатируются в неизбежных условиях риска и неопределенности. Концепция риска основана на определении текущих состояний элементов системы и условий возникновения и развития угроз при чрезвычайных, аварийных и катастрофических ситуациях, качественном и количественном описании сценариев и последствий достижения предельных состояний с возникновением аварий и катастроф [22].

Модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз. В рамках исследований киберситуационной осведомленности автором предлагается модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз, на основе байесовских сетей доверия (БСД). Модель строится в соответствии с типовой схемой атаки на технологический сегмент сети [8], включающей три основных этапа:

1. Проникновение в корпоративную информационную систему (КИС).
2. Проникновение из КИС в технологический сегмент (ТС) локальной вычислительной сети (ЛВС).
3. Атака на целевой актив.

На основе модели осуществляется вероятностный вывод и определяются вероятности киберугроз на каждом этапе. Вероятностный вывод требует совместного распределения вероятностей, вследствие чего возникает проблема экспоненциальной сложности с ростом количества переменных. Для решения подобной проблемы создаются модели байесовской сети доверия, разбивающие сложное распределение вероятностей на ряд простых узлов, что снижает проблематичность получения знаний и сложность вероятностного вывода [23].

В статье рассматривается уровень КСО как способ измерения ситуационной осведомленности в киберсреде. На основе структурирования знаний с использованием фрактального стратифицированного подхода [14] и онтологического инжиниринга [2] разработана модель сценариев ЭкС в энергетике, вызванных киберугрозами:

$$M = \{A, V, T, W, C, F\}, \quad (1)$$

где A – множество активов информационно-технологической системы энергетического объекта (аппаратно-программные, программные, протоколы и пр.), V – множество всех обнаруженных критических уязвимостей активов рассматриваемой ЛВС, T – множество киберугроз активов ЛВС, W – множество техногенных угроз ЭБ, вызванных киберугрозами T, C– множество последствий реализации угроз, F – множество взаимосвязей между критическими активами, уязвимостями активов ЛВС, угрозами и последствиями реализации угроз, представленных в виде продукционных правил «ЕСЛИ-ТО».

Далее рассмотрим каждый компонент модели подробнее. Множество активов информационно-технологической системы энергетического объекта A включает подмножество активов ЛВС и технологической инфраструктуры:

$$A = \{A^E, A^I\}, \quad (2)$$

$$A^E = \{a_1^E, a_2^E, \dots, a_k^E\}, \quad (3)$$

$$A^T = \{a_1^I, a_2^I, \dots, a_l^I\}, \quad (4)$$

где A^{E} – множество активов ЛВС, A^{I} – множество активов технологической инфраструктуры (ТехИ) (энергетические объекты), $a_1^E, a_2^E, \dots, a_k^E$ – активы ЛВС, $a_1^I, a_2^I, \dots, a_l^I$ – активы ТехИ.

Каждый актив a_i^E содержит набор критических уязвимостей или, иными словами, каждой критической уязвимости из набора уязвимостей ставится в соответствие конкретный актив ЛВС, так что:

$$F_{a_i^E}^{V_i}: V_i \longrightarrow a_i^E, \quad (5)$$

$$V_i = \{v_1, v_2 \ \dots, v_m\}, V_i \subset V, \quad (6)$$

где $F_{a_i^E}^{V_i}$ – отображение взаимосвязи между активом ЛВС a_i^E и набором обнаруженных критических уязвимостей V_i актива.

Множество киберугроз T представлено двумя подмножествами:

$$T = \{T^V, T^W\}, \quad (7)$$

где T^V – множество киберугроз, инициирующих критические уязвимости, T^W – множество киберугроз, спровоцированных инициирующими киберугрозами T^V.

Каждая уязвимость v_i может быть использована одной или более инициирующей киберугрозой, т.е.:

$$T_i^V = \{t_1^V, t_2^V, \dots, t_h^V\}, T_i^V \subset T^V, \quad (8)$$

$$F_{v_i}^{T_i^V}: T_i^V \longrightarrow v_i, \quad (9)$$

где $t_1^V, t_2^V, \dots, t_h^V$ – набор киберугроз, которые могут инициировать уязвимость v_i, $F_{v_i}^{T_i^V}$ – отображение взаимосвязи между уязвимостью v_i и набором инициирующих её киберугроз.

В свою очередь, инициирующие киберугрозы влекут реализацию других киберугроз т.е. цепочки киберугроз (вектора атак), представленных, как:

$$T_i^W = \{t_1^W, t_2^W, \dots, t_z^W\}, T_i^W \subset T^W, \quad (10)$$

$$F_{T_i^V}^{t_i^W}: t_i^W \longrightarrow T_i^V, \quad (11)$$

где $t_1^W, t_2^W, \dots, t_z^W$ – набор киберугроз, спровоцированных киберугрозой t_i^V, $F_{t_i^V}^{T_i^W}$ – отображение взаимосвязи между инициирующей угрозой и набором спровоцированных киберугроз.

Кибернетические угрозы способны вызывать техногенные угрозы на объекте, которые также являются угрозами энергетической безопасности:

$$W = \{w_1, w_2, \dots, w_u\}, \quad (12)$$

$$F_W^{T_i}: T_i \longrightarrow W, \quad (13)$$

где W – множество техногенных угроз ЭБ, вызванных киберугрозами T, $F_W^{T_i}$ – отображение взаимосвязи между вектором атаки и множеством техногенных угроз ЭБ W, рассматриваемым в модели как вектор киберугрозы.

Техногенные угрозы ЭБ на объекте могу привести к неблагоприятным последствиям, нарушающим функционирование объекта:

$$C = \{c_1, c_2, \dots, c_q\}, \quad (14)$$

$$F_W^{C_k}: C_k \longrightarrow W, \tag{15}$$

где C – множество последствий реализации угроз, $F_T^{C_k}$ – отображение взаимосвязи между множеством техногенных угроз ЭБ и последствиями реализации угроз.

Множество взаимосвязей модели описывается следующим образом:

$$F = \left\{ F_{a_i^E}^{V_i}, F_{v_i}^{T_i^V}, F_{T_i^V}^{t_i^W}, F_W^{T_i}, F_W^{C_k} \right\}, \tag{16}$$

где $F_{a_i^E}^{V_i}, F_{v_i}^{T_i^V}, F_{T_i^V}^{t_i^W}, F_W^{T_i}, F_W^{C_k}$ определены в формулах (9), (11), (13), (15).

Численный метод определения уровня КСО энергетического объекта. Определять уровень КСО предлагается с использованием описанной выше модели, по формуле:

$$L = \frac{Z}{2^n - 1}, \tag{17}$$

где L – уровень КСО энергетического объекта, Z – количество рассчитанных сценариев ЭкС в энергетике, вызванных киберугрозами, $2^n - 1$ – общее количество таких сценариев, где $n = |V| + |T| + |W|$. Значения V, T, W введены ранее в формулах (6)-(7), (12).

Численный метод реализуется алгоритмом, представленным на рис 1 а. Блоки 4-7 алгоритма на рис. 1 а представлены детализированным алгоритмом на рис. 1 б.

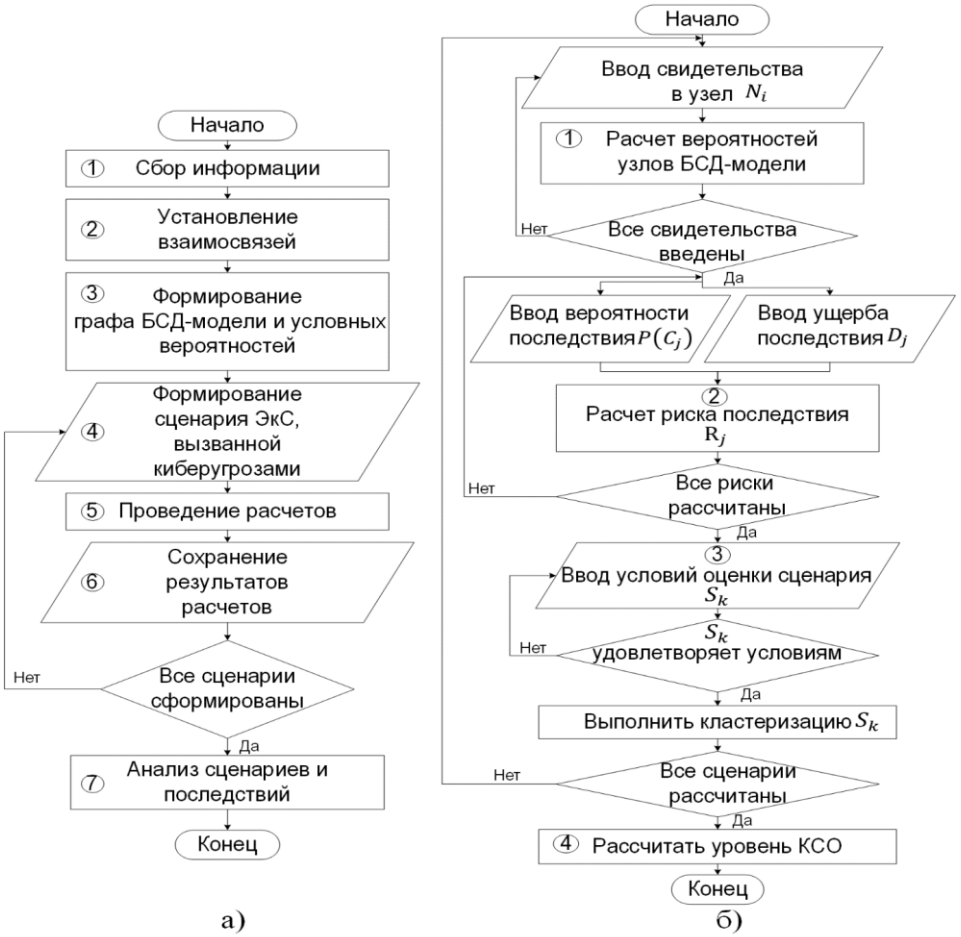

Рис. 1. а) алгоритм определения уровня КСО энергетического объекта, б) детализированный алгоритм блоков 4-7 алгоритма определения уровня КСО

Комментарий к рис 1 а. Блоки 1-3 соответствуют сбору информации, который заключается в определении множеств активов A формула (2), критических уязвимостей V (6), киберугроз T (7-11), W – техногенных угроз ЭБ (12), C – последствий реализации угроз (14), установлении взаимосвязей F (16).

Блок 4 представляет формирование графа БСД-модели и таблиц условных вероятностей (ТУВ) его узлов (для всех типов узлов в соответствии с M (1) – моделью сценариев ЭкС в энергетике, вызванной киберугрозами для расчета сценария). Начальные вероятностные характеристики (ТУВ) определяются на основе экспертных или статистических данных.

Для проведения расчетов (блоки 5-6) требуется вычислить вероятность последствий для каждого сценария, кластеризовать сценарии в соответствии с критериями кластеризации и определить уровень КСО. Сценарий описывается как:

$$S_k^{\mathrm{C}} = \{S_1^{\mathrm{C}}, S_2^{\mathrm{C}}, \dots, S_j^{\mathrm{C}}\}, \tag{18}$$

где S_k^{C} – множество кластеризованных сценариев ЭкС в энергетике, вызванных киберугрозами (все сценарии разбиваются на три кластера: норма, предкризис, кризис [6]), $k = \overline{1,3}$. Принимается, что существует взаимно-однозначное соответствие между сценарием S_j^{C} и вероятностью его последствия $P(c_q^S)$.

Анализ сценариев и последствий (блок 7) осуществляется путем анализа распределения рисков отдельных сценариев по кластерам, сопровождается описанием рисков R:

$$R = \{T, V, W, C, D\}, \tag{19}$$

где значения T, V, W, C введены ранее в (7-15), D – ущерб последствия сценария S^C.

Комментарий к рис. 1 б. Расчет вероятностей (блок 1) выполняется по формулам:

$$\begin{gathered} P(N_j|E_i = True) = \sum_{j=1}^{n} P(E_i = True) \times P(N_j|E_i = True), \\ P(N_j|E_i = False) = \sum_{j=1}^{n} P(E_i = False) \times P(N_j|E_i = False), \\ N_j \in N\ , \end{gathered} \tag{20}$$

где N – множество всех узлов графа БСД-модели, E_i – узел графа БСД-модели, в который введено свидетельство, N_j – множество дочерних узлов узла E_i, $i = \overline{1, |N| - |C|}$, $n = \overline{1, |N_j|}$, C введено ранее в (14).

Количественная оценка рисков последствий сценария S_j^{C} (блок 2) выражается в вычислении вероятностного ущерба по формуле:

$$R_j = P(C_j) \times D_j, \tag{21}$$

где вероятность P является функцией G от сценария S^C: $P(C_j) = G(S^C)$, $\mathrm{P}(C_j)$ – вероятность последствия сценария S_j^C, рассчитываемая по формулам (20), D_j – ущерб от реализации киберугроз этого сценария.

Условия оценки сценариев ЭкС, вызванных киберугрозами (блок 3), имеют вид:

$$0 \le P(C_j) \times D_{C_j} \le l_1, \tag{22}$$

$$l_1 \le P(C_j) \times D_{C_j} \le l_2, \tag{23}$$

$$l_2 \le P(C_j) \times D_{C_j}, \tag{24}$$

$$0 \le P(C_j) \le 1\ , \tag{25}$$

$$0 \le D_{C_j} \le D_m, \tag{26}$$

где l_1, l_2 – критерии кластеризации сценариев ЭкС, вызванных киберугрозами, D_m – максимальный ущерб.

Сценарии, удовлетворяющие условиям (22), (25), (26) считаем незначительными (норма), удовлетворяющие условиям (23), (25), (26) считаем соответствующими среднему уровню опасности (предкризис), удовлетворяющие условиям (24), (25), (26) – опасными (кризис).

Определение уровня КСО энергетического объекта (блок 4, рис. 1б) осуществляется по формуле (17).

Заключение. В статье приведены определения киберситуационной осведомленности, представлены модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз, предложенная на основе выполненного ранее структурирования знаний с использованием фрактального стратифицированного подхода и онтологического инжиниринга, и численный метод определения уровня КСО энергетического объекта. Реализация предложенных модели и численного метода определения уровня КСО энергетического объекта выполнена в рамках разработки интеллектуального программного комплекса ИПК «ОКО» для анализа киберситуационной осведомленности энергетического объекта.

Благодарности. Работа выполнена в рамах выполнения проекта по госзаданию ИСЭМ СО РАН АААА-А17-117030310444-2 (проект №349-2016-0005) и при частичной финансовой поддержке грантов РФФИ №19-57-04003, № 19-07-00351, №18-07-00714, 20-010-00204.

СПИСОК ЛИТЕРАТУРЫ

1. APT-атаки на топливно-энергетический комплекс России: обзор тактик и техник / Аналитические статьи Positive Technologies. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019/ (дата обращения: 15.11.2020).
2. Гаськова Д.А., Массель А.Г. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов // Онтология проектирования. 2019. Т. 9. №2 (32). С. 225-238.
3. Кибератаки на системы АСУ ТП в энергетике в Европе. Первый квартал 2020 года / Отчеты Kaspersky ICS CERT. Режим доступа: https://ics-cert.kaspersky.ru/reports/2020/09/03/cyberthreats-for-ics-in-energy-in-europe-q1-2020/ (дата обращения: 15.11.2020).
4. 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.
5. Массель Л.В., Иванов Р.А., Массель А.Г. Моделирование этапов принятия решений на основе сетецентрического подхода // Вестник ИрГТУ. 2013. №10(81). С.16-22.
6. Массель Л.В., Массель А.Г. Технологии и инструментальные средства интеллектуальной поддержки принятия решений в экстремальных ситуациях в энергетике // Вычислительные технологии. 2013. Т. 18. № S1. С. 37-44.
7. Об утверждении Доктрины энергетической безопасности Российской Федерации / Указ Президента Российской Федерации от 13 мая 2019 года № 216. Режим доступа: https://minenergo.gov.ru/system/download-pdf/14766/9694114766 (дата обращения 15.11.2020).
8. Промышленные компании: векторы атак/ Аналитические статьи Positive Technologies. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/ (дата обращения 15.11.2020).
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.

10. Eckhart M., Ekelhart A., Weippl E. Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins // Proceedings of the 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). 2019. Pp. 1222-1225. DOI:10.1109/etfa.2019.8869197.

11. Endsley M.R. Situation awareness global assessment technique (SAGAT) // Proceedings of the IEEE 1988 National Aerospace and Electronics Conference. 1988. Pp. 789-795. DOI:10.1109/naecon.1988.195097.

12. Endsley M.R. Theoretical underpinnings of situation awareness: A critical review. In: Endsley M.R, Garland D.J. Situation awareness analysis and measurement. 2000. Pp. 3-32.

13. Frank U., Brynielsson J. Cyber Situational Awareness – A systematic review of literature // Computer Security. 2014. Vol. 46. Pp. 18–31. DOI: 10.1016/j.cose.2014.06.008.

14. Gaskova D. Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security // Proceedings of the VIth International Workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security (IWCI 2019)". Publisher: Atlantis Press. 2019. Irkutsk: MESI SB RAS. Pp. 179-183. DOI:10.2991/iwci-19.2019.31.

15. Irmak E., Erkek I. An overview of cyber-attack vectors on SCADA systems // Proceedings of 6th International Symposium on Digital Forensic and Security (ISDFS). 2018. DOI:10.1109/isdfs.2018.8355379.

16. ISO/IEC 27032:2012 ISO standard of Information technology. Security techniques. Guidelines for cybersecurity. Режим доступа: https://www.iso.org/ru/standard/44375.html (дата обращения 15.11.2020).

17. MITRE Capabilities overviews. Режим доступа: https://www.mitre.org/capabilities/cybersecurity/situation-awareness (дата обращения 15.11.2020).

18. National Institute of Standards and Technology (NIST) Glossary. Режим доступа: https://csrc.nist.gov/glossary (дата обращения 15.11.2020).

19. Okolica J.S., McDonald J.T., Peterson G.L., Mills R.F., Haas M.W. Developing Systems for Cyber Situational Awareness // Proceedings of the 2nd Cyberspace Research Workshop. Shreveport. Louisiana. 2009.

20. Pappaterra M. J., Flammini F. A Review of Intelligent Cybersecurity with Bayesian Networks // Proceedings of IEEE International Conference on Systems, Man and Cybernetics (SMC). Bari. Italy. 2019. Pp. 445-452. DOI:10.1109/smc.2019.8913864.

21. T-REC-X.1205 – ITU-T: Overview of cybersecurity. Режим доступа: https://www.itu.int/rec/T-REC-X.1205-200804-I (дата обращения 15.11.2020).

22. Yacov Y. Haimes. Systems-based risk analysis. In: Bostrom N., Cirkovic M.M. Global Catastrpphic Risks. Oxford. 2008. Pp. 146-163.

23. Zhang Q., Zhou C., Xiong N., Qin Y., Li X., Huang S. Multimodel-Based Inci-dent Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems // Proceedings of IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2016. Vol. 46. № 10. Pp. 1429-1444. DOI: 10.1109/TSMC.2015.2503399.

UDK 04.89:519.226.3

METHOD FOR DETERMINING THE LEVEL OF CYBER SITUATIONAL AWARENES ON ENERGY FACILITIES

Daria A. Gaskova
Junior Researcher, e-mail: gaskovada@gmail.com,
Melentiev Energy Systems Institute of
Siberian Branch of the Russian Academy of Sciences,
130, Lermontov Str., 664033, Irkutsk, Russia.

Annotation. The article describes the research direction of situational awareness in the cyber environment on energy facilities. A model based on a Bayesian Belief Network and a numerical method for determining cyber situational awareness are proposed to increase awareness of the cyber environment state on such facilities. The model is based on causal relationships between the vulnerabilities of the local area network and possible cyber threats, presented in the form of vectors of penetration into the network, vectors of the development of cyber attacks and attack vectors on the target asset, combined in scenarios. The work focuses on scenarios, the consequences of which can be regarded as extreme situations in the energy sector caused by cyber threats.

Keywords: Bayesian Belief Network, emergency situation in the energy sector, cyber threats.

References

1. APT-ataki na toplivno-energeticheskij kompleks Rossii: obzor taktik i tekhnik [APT attacks to Russian energy sector: review of tactics and techniques] / Analytics of Positive Technologies. Avalible at: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019 accessed 15.11.2020 (in Russian).
2. Gaskova D.A., Massel A.G. Ontologicheskij inzhiniring dlya razrabotki intellektual'noj sistemy analiza ugroz i ocenki riskov kiberbezopasnosti energeticheskih obektov [Ontological engineering for the development of the intelligent system for threats analysis and risk assessment of cybersecurity in energy facilities] // Ontologiya proektirovaniya = Ontology of Designing. 2019. Vol. 9. Issue 2(32). Pp. 225-238 (in Russian).
3. Kiberataki na sistemy ASU TP v energetike v Evrope [Cyberattacks on ICS in energy in in Europe] / Reports of Kaspersky ICS CERT. Avalible at: https://ics-cert.kaspersky.ru/reports /2020/09/03/cyberthreats-for-ics-in-energy-in-europe-q1-2020 accessed 15.11.2020 (in Russian).
4. Massel L.V., Voropay N.I, Senderov S.M, Massel A.G. Kiberopasnost' kak odna iz strategicheskih ugroz energeticheskoj bezopasnosti [Cyber danger as one of the strategic threats to russia's energy security] // Voprosy kiberbezopasnosti = Cybersecurity issues. 2016. №. 4(17). Pp. 2-10 (in Russian).
5. Massel L.V., Ivanov R.A., Massel A.G. Modelirovanie etapov prinyatiya reshenij na osnove setecentricheskogo podhoda [Decision-making stages modeling based on network-centric approach] // Vestnik IrGTU = Proceedings of ISTU. 2013. № 10(81). Pp. 16-22 (in Russian).

6. Massel L.V., Massel A.G. Tekhnologii i instrumental'nye sredstva intellektual'noj podderzhki prinyatiya reshenij v ekstremal'nyh situaciyah v energetike [Technologies and tools for intelligent decision-making support in extreme situations in the energy sector] // Vychislitel'nye tekhnologii = Computational Technologies. 2013. Vol. 18. № S1. Pp. 37-44 (in Russian).

7. Ob utverzhdenii Doktriny energeticheskoj bezopasnosti Rossijskoj Federacii [On approval of the Energy Security Doctrine of the Russian Federation] / Ukaz Prezidenta Rossijskoj Federacii ot 13 maya 2019 goda no. 216 = Decree of the President of the Russian Federation of May 13. 2019. № 216. Avalible at: https://minenergo.gov.ru/system/download-pdf/14766/9694114766, accessed 15.11.2020 (in Russian).

8. Promyshlennye kompanii: vektory atak [Industrial companies: attack vectors] / Analytics of Positive Technologies. Avalible at: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018 accessed 15.11.2020 (in Russian).

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.

10. Eckhart M., Ekelhart A., Weippl E. Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins // Proceedings of the 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). 2019. Pp. 1222-1225. DOI:10.1109/etfa.2019.8869197.

11. Endsley M.R. Situation awareness global assessment technique (SAGAT) // Proceedings of the IEEE 1988 National Aerospace and Electronics Conference. 1988. Pp. 789-795. DOI:10.1109/naecon.1988.195097.

12. Endsley M.R. Theoretical underpinnings of situation awareness: A critical review. In: Endsley M.R, Garland D.J. Situation awareness analysis and measurement. 2000. Pp. 3-32.

13. Frank U., Brynielsson J. Cyber Situational Awareness – A systematic review of literature // Computer Security. 2014. Vol. 46. Pp. 18–31. DOI: 10.1016/j.cose.2014.06.008.

14. Gaskova D. Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security // Proceedings of the VIth International Workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security (IWCI 2019)". Publisher: Atlantis Press. 2019. Irkutsk: MESI SB RAS. Pp. 179-183. DOI: 10.2991/iwci-19.2019.31.

15. Irmak E., Erkek I. An overview of cyber-attack vectors on SCADA systems // Proceedings of 6th International Symposium on Digital Forensic and Security (ISDFS). 2018. DOI: 10.1109/isdfs.2018.8355379.

16. ISO/IEC 27032:2012 ISO standard of Information technology. Security techniques. Guidelines for cybersecurity. Режим доступа: https://www.iso.org/ru/standard/44375.html (дата обращения 15.11.2020).

17. MITRE Capabilities overviews. Режим доступа: https://www.mitre.org/capabilities/cybersecurity/situation-awareness (дата обращения 15.11.2020).

18. National Institute of Standards and Technology (NIST) Glossary. Режим доступа: https://csrc.nist.gov/glossary (дата обращения 15.11.2020).

19. Okolica J.S., McDonald J.T., Peterson G.L., Mills R.F., Haas M.W. Developing Systems for Cyber Situational Awareness // Proceedings of the 2nd Cyberspace Research Workshop. Shreveport. Louisiana. 2009.
20. Pappaterra M. J., Flammini F. A Review of Intelligent Cybersecurity with Bayesian Networks // Proceedings of IEEE International Conference on Systems, Man and Cybernetics (SMC). Bari. Italy. 2019. Pp. 445-452. DOI:10.1109/smc.2019.8913864.
21. T-REC-X.1205 – ITU-T: Overview of cybersecurity. Режим доступа: https://www.itu.int/rec/T-REC-X.1205-200804-I (дата обращения 15.11.2020).
22. Yacov Y. Haimes. Systems-based risk analysis. In: Bostrom N., Cirkovic M.M. Global Catastrpphic Risks. Oxford. 2008. Pp. 146-163.
23. Zhang Q., Zhou C., Xiong N., Qin Y., Li X., Huang S. Multimodel-Based Inci-dent Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems // Proceedings of IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2016. Vol. 46. №. 10. Pp. 1429-1444. DOI: 10.1109/TSMC.2015.2503399.