Научная статья
УДК 004.942
https://doi.org/10.24143/2072-9502-2025-3-70-77
EDN THOUVO

Особенности оценки и прогнозирования уровня защищенности объектов критической инфраструктуры с компонентами технологии Интернета вещей на основе методов теории катастроф

Игорь Витальевич Котенко, Дмитрий Сергеевич Левшун, Игорь Борисович Паращук ✉

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, Россия, shchuk@rambler.ru ✉

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Санкт-Петербург, Россия

Аннотация. Объектом исследования является новый методологический подход к оценке и прогнозированию уровня защищенности сложных киберфизических объектов, а также к построению и применению моделей и методов теории катастроф как к новому математическому и методологическому инструментарию повышения достоверности оценки и прогноза уровня защищенности объектов критической инфраструктуры (ОКИ), использующих технологию Интернета вещей (ТИВ) в интересах своевременного предупреждения об опасности и принятия превентивных мер для повышения их информационной безопасности. Предложенный подход основан на известных методах теории катастроф, в частности на методах исследования бифуркаций, позволяющих реализовать оценку и прогнозирование уровня защищенности объектов такого класса с использованием алгоритмов идентификации и верификации граничного и потенциально катастрофичного состояния (уровня) защищенности при плавно нарастающих изменениях параметров внешних условий, например плавных изменениях интенсивности обнаруживаемых признаков компьютерных атак. При этом алгоритм оценки и прогнозирования уровня защищенности с точки зрения математики теории катастроф и теории пространств состояния рассматривается как анализ процесса перехода уровня защищенности объекта критической инфраструктуры из состояния в состояние. Произведен подробный анализ отличительных черт этого подхода, определяющих целесообразность и условия его применения для оценки и прогнозирования потенциально опасного, тревожного уровня защищенности ОКИ, использующих ТИВ. Выработана и детально изложена последовательность вычислений и аналитические выражения для расчета оценочных значений состояния (уровня) защищенности для различных категорий признаков потенциальных компьютерных атак. Приведены результаты экспериментальных вычислений для примера оценки и прогнозирования состояния (уровня) защищенности с учетом интенсивности поступления (выявления) различных признаков компьютерных атак на ОКИ, использующие ТИВ.

Ключевые слова: объект критической инфраструктуры, технология Интернета вещей, компьютерная атака, защищенность, оценка, прогноз, признак, теория катастроф, бифуркация, интенсивность

Благодарности: работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.

Для цитирования: *Котенко И. В., Левшун Д. С., Паращук И. Б.* Особенности оценки и прогнозирования уровня защищенности объектов критической инфраструктуры с компонентами технологии Интернета вещей на основе методов теории катастроф // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2025. № 3. С. 70–77. https://doi.org/10.24143/2072-9502-2025-3-70-77. EDN THOUVO.

Original article

Features of assessing and forecasting the critical infrastructure facilities level of security with components of the Internet of Things technology based on catastrophe theory methods

Igor V. Kotenko, Dmitry S. Levshun, Igor B. Parashchuk ✉

St. Petersburg Federal Research Center of the Russian Academy of Sciences,
Saint Petersburg, Russia, shchuk@rambler.ru ✉

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
Saint Petersburg, Russia

Abstract. The object of the study is a new methodological approach to assessing and predicting the level of protection of complex cyber-physical objects, as well as to the construction and application of models and methods of catastrophe theory, as a new mathematical and methodological tool for increasing the reliability of the assessment and forecast of the level of protection of critical infrastructure objects (CIO) using the Internet of Things technology (ITT) in the interests of timely warning of danger and taking preventive measures to improve their information security. The proposed approach is based on well-known methods of catastrophe theory, in particular, on the methods of studying bifurcations that allow implementing the assessment and forecasting of the level of protection of objects of this class using algorithms for identifying and verifying the boundary and potentially catastrophic state (level) of protection with smoothly increasing changes in the parameters of external conditions, for example, smooth changes in the intensity of detected signs of computer attacks. In this case, the algorithm for assessing and predicting the security level, from the point of view of the mathematics of catastrophe theory and the theory of state spaces, is considered as an analysis of the process of transition of the security level of a critical infrastructure object from state to state. A detailed analysis of the distinctive features of this approach is made, determining the feasibility and conditions of its application for assessing and predicting a potentially dangerous, alarming level of security of CIO using ITT. A sequence of calculations and analytical expressions for calculating the estimated values of the security state (level) for various categories of signs of potential computer attacks are developed and described in detail. The results of experimental calculations are given for an example of assessing and predicting the security state (level) taking into account the intensity of receipt (detection) of various signs of computer attacks on CIO using ITT.

Keywords: critical infrastructure object, Internet of Things technology, computer attack, security, assessment, forecast, sign, catastrophe theory, bifurcation, intensity

Acknowledgment: the work was partially supported by the FFZF-2025-0016 budget theme.

For citation: Kotenko I. V., Levshun D. S., Parashchuk I. B. Features of assessing and forecasting the critical infrastructure facilities level of security with components of the Internet of Things technology based on catastrophe theory methods. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2025;3:70-77. (In Russ.). https://doi.org/10.24143/2072-9502-2025-3-70-77. EDN THOUVO.

Введение

Современные объекты критической инфраструктуры (ОКИ) – это защищенные от внешних и внутренних дестабилизирующих воздействий подсистемы, отдельные важные предприятия, сети систем жилищно-коммунальной сферы, базовые компоненты и структуры поддержки существования и функционирования, а также автоматические, роботизированные и автоматизированные системы связи и управления ими, функционирующие в ключевых сферах здравоохранения, науки, транспорта, обороны, телекоммуникаций, энергетики, банковской и иных важнейших областях жизнедеятельности общества и государства [1–3]. Вместе с тем широкое внедрение современной технологии Интернета вещей (ТИВ) для коммуникации ОКИ между собой и для управления своими компонентами вольно либо невольно создает предпосылки для возможного появления и практической реализации широкого спектра угроз информационной безопасности объектов такого класса и предоставляемых ими критических информационных и телекоммуникационных ресурсов [4–6].

Специфика ТИВ, наряду с неоспоримыми достоинствами, обуславливает и недостатки их применения, к перечню которых специалисты, например, критических энергетических или железнодорожных транспортных сфер относят риски и угрозы информационной безопасности, которые связаны с компьютерными атаками на инфраструктуру ОКИ, направленными на незаконный доступ к данным, циркулирующим внутри или между такими объектами, на нарушение цифровых транзакций или модификацию (повреждение) информации [7–10].

Опасный характер угроз информационной безопасности для ОКИ, использующих ТИВ, обуславливает необходимость комплексной и многокритериальной оценки уровня их защищенности. Помимо этого ряд обстоятельств позволяет выдвинуть гипотезу о том, что подобная оценка может и должна быть не только интервальной, но и прогнозной, упреждающей, проактивной, чтобы заранее подготовиться к нарастающему кризису информационной безопасности, когда защищенность критических объектов постепенно достигает угрожающего, экстремально-опасного уровня, чтобы предусмотреть ответные превентивные меры защиты в рамках существующих возможностей подсистем управления информационной безопасностью [11–14].

Перспективным направлением определения и доказательства жизнеспособности этой гипотезы, на наш взгляд, является разработка алгоритмов оценки и прогнозирования потенциально опасного уровня защищенности ОКИ, использующих ТИВ, на базе методологических и математических инструментов теории катастроф. Под теорией катастроф понимается теория, описывающая скачкообразные изменения, возникающие в виде внезапного ответа системы на плавное изменение условий ее функционирования.

Применение методов теории катастроф для нашей задачи позволит учитывать при прогнозировании угрожающего уровня защищенности динамику возможного скачкообразного изменения переменных состояния (критических параметров) защи-

щенности ОКИ в ответ на плавное изменение внешних и внутренних воздействий на информационную безопасность объектов такого класса [15–17].

Таким образом, своевременной и важной целью работы является создание и анализ особенностей новой методики решения задачи построения и практического применения алгоритмов оценки и прогнозирования потенциально опасного уровня защищенности ОКИ, использующих ТИВ, задачи создания достоверных и оперативных механизмов и математических методов предсказания предполагаемо катастрофичного уровня (степени, состояния) защищенности объектов такого класса.

Эти достоверные и оперативные механизмы и методы должны быть основаны на идентификации и верификации граничного и потенциально угрожающего уровня (состояния) защищенности при плавно нарастающих негативных изменениях параметров внешних условий, например плавных изменениях интенсивности поступающих (идентифицируемых) признаков компьютерной атаки.

Решение подобной задачи позволит повысить достоверность оценки и прогноза уровня защищенности подобных сложных критических объектов в интересах своевременного предупреждения об опасности и принятия мер для повышения их защиты в рамках принятой политики информационной безопасности.

Методологические аспекты оценки и прогнозирования уровня защищенности объектов критической инфраструктуры, использующих Интернет вещей

Теория катастроф представляет собой комплекс взаимосвязанных и дополняющих друг друга математических средств и методов (иногда называемых элементами теории особенностей), представляющих собой обобщение исследования функций на максимумы и минимумы. Именно потому, что минимумы и максимумы представляют собой критические точки функции параметров сложной динамической системы, например функции параметров информационной безопасности, которые во многом определяют смену состояний защищенности (поведение, тренд) такой системы, методы теории катастроф могут быть применены для задачи оценки и прогнозирования защищенности критических объектов [15, 16].

Одним из наиболее распространенных приложений теории катастроф является понятие бифуркации, под которым принято понимать качественное изменение поведения динамической системы при плавном и бесконечно малом изменении ее параметров. Иными словами, в теории катастроф бифуркация представляется как скачкообразная качественная перестройка системы при плавном изменении параметров [15–17].

Таким образом, анализ релевантных работ и опыта безопасной практической эксплуатации сложных ОКИ показал, что применение методов теории катастроф (исследования бифуркаций) для задач оценки и прогнозирования уровня защищенности ОКИ, использующих ТИВ, может и должно обеспечить реальную возможность идентификации и верификации потенциально опасных, граничных и предаварийных (катастрофичных) уровней (состояний) защищенности подобных объектов при плавных и малых изменениях значений параметров их информационной безопасности, обусловленных внешними условиями и управляющими воздействиями. Примером таких условий могут служить плавные изменения интенсивности поступающих (идентифицируемых) признаков компьютерных атак на объекты такого класса.

С точки зрения формального описания концептуальных (на уровне идей и принципов) аспектов применения методов теории катастроф (в рамках исследования бифуркаций) для задач оценки и прогнозирования физический смысл параметров внешних условий и управляющих воздействий, влияющих на поведение, на плавное изменение значений параметров информационной безопасности, может быть представлен посредством статистического анализа и определения, например, соответствующих значений интенсивности возникновения (выявления) признаков компьютерной атаки $\lambda_{п.к.а}$ на ОКИ, использующие ТИВ.

Такая интенсивность $\lambda_{п.к.а}$ представляет собой количество $\omega_{п.к.а}$ разнообразных признаков компьютерной атаки на ОКИ, использующие ТИВ, фиксируемых за единицу времени наблюдения $\tau_{наб}$:

$$\lambda_{п.к.а} = \omega_{п.к.а} / \tau_{наб},$$

где $\lambda_{п.к.а} = 1, 2, ..., \Lambda$.

Признаками компьютерной атаки на ОКИ, использующие ТИВ, могут быть:

– признаки сканирования портов компьютера или сервера;

– резкое падение производительности компьютера;

– постоянное обращение к жесткому диску;

– сбои в учетных записях; регулярно возникающие сообщения об ошибках;

– «подозрительное» поведение браузера, например самопроизвольная замена баннеров на сайтах;

– недоступные или исчезнувшие файлы или папки;

– появление незнакомых файлов или приложений;

– нотификации (без согласия пользователя) об удаленном подключении;

– появление писем или сообщений, которые не были отправлены, и др.

Пусть общее число Q следующих друг за другом временных интервалов наблюдения $\tau_{\text{наб}}$ будет обозначено как q, где q = 1, 2, ..., Q. При этом общее число Q следующих друг за другом временных интервалов наблюдения $\tau_{\text{наб}}$ за состоянием (уровнем) защищенности ОКИ, использующих ТИВ, определяет «глубину прогнозирования» этого уровня.

В рамках методов теории катастроф общее количество значений интенсивности возникновения (выявления) признаков компьютерной атаки $\lambda_{\text{п.к.а}}$ на ОКИ, использующие ТИВ, равно Λ, и эти значения могут быть записаны в виде множества [15, 16]

$$\Lambda_Q = \left\{ \lambda^1_{\text{п.к.а}}(\tau_{\text{наб}});\ \lambda^2_{\text{п.к.а}}(\tau_{\text{наб}}+1);\ \ldots;\ \lambda^q_{\text{п.к.а}}(\tau_{\text{наб}}+q);\ \ldots;\ \Lambda_{Q-1}(\tau_{\text{наб}}+(Q-1)) \right\},$$

где каждый q-й элемент множества, кроме $\Lambda_{Q-1}(\tau_{\text{наб}}+(Q-1))$, является подмножеством Λ_Q и имеет физический смысл превышения критического порога защищенности с точки зрения потенциально катастрофического превышения интенсивности возникновения компьютерной атаки.

Более того, что особенно важно, это говорит о высокой вероятности перехода уровня защищенности в опасное (катастрофичное) состояние на следующем временном интервале ($\tau_{\text{наб}}$ + 1) наблюдения и функционирования ОКИ, использующих ТИВ.

Для численного решения задач оценки и прогнозирования уровня защищенности или, для нашего конкретного примера, для прогностического расчета и сравнения значений интенсивности возникновения (выявления) признаков компьютерной атаки $\lambda_{\text{п.к.а}}$ на ОКИ, использующие ТИВ, при плавных изменениях параметров внешних условий, необходимо осуществлять пошаговый контроль, проводить последовательную и методичную идентификацию и верификацию потенциально угрожающих, граничных и экстремально-опасных состояний (уровней) защищенности.

Методологические особенности процедур верификации катастрофичных состояний (уровней) защищенности объектов критической инфраструктуры, использующих Интернет вещей

В рамках теории катастроф (исследования бифуркаций) идентификация уровня защищенности может быть осуществлена путем пошагового (на каждом шаге, т. е. на каждом q-м временном интервале ($\tau_{\text{наб}}$ + q) наблюдения, прогнозной оценки и сравнения значений каждого q-го элемента $\lambda^q_{\text{п.к.а}}$ множества Λ_Q с целью определения наличия или отсутствия возможного превышения этими значениями допустимого порога интенсивности поступления (выявления) признаков компьютерной атаки, определяемого как

$$\lambda^q_{\text{п.к.а}}(\tau_{\text{наб}}+q) \underset{<}{\overset{>}{}} \Lambda_Q, \qquad (1)$$

где $\underset{<}{\overset{>}{}}$ – символ сравнения, а Λ_Q – допустимое значение интенсивности поступления (выявления) признаков компьютерной атаки на q-м временном интервале ($\tau_{\text{наб}}$ + q) наблюдения за состоянием параметров защищенности, при превышении которого уровень защищенности ОКИ, использующих ТИВ, с большой вероятностью перейдет в граничное и потенциально катастрофическое состояние из любого другого состояния.

Такая формулировка верна и имеет право на применение в предположении, что в целом алгоритм оценки и прогнозирования уровня защищенности, с точки зрения математики пространств состояния, можно рассматривать как процесс перехода уровня защищенности ОКИ из состояния в состояние.

В рамках контроля уровня защищенности и определения, по сути, события бифуркации, на начальном (первом) шаге наблюдения, для «стартового» временного интервала оценки и прогнозирования, выражение для контроля интенсивности поступления признаков компьютерной атаки (1) имеет вид

$$\lambda^1_{\text{п.к.а}}(\tau_{\text{наб}}) \underset{<}{\overset{>}{}} \Lambda_1.$$

Превышение на одном из последующих ($\tau_{\text{наб}}$ + 1), ($\tau_{\text{наб}}$ + 2), ... и т. д. временных интервалов любым значением интенсивности $\lambda^q_{\text{п.к.а}}$ данного порога характеризует начало медленного, плавного, чаще негативного (с точки зрения защищенности) изменения параметров внешних условий.

С точки зрения методов теории катастроф и ее подраздела – исследования бифуркаций – верификация граничных и потенциально катастрофичных состояний (уровней) защищенности представляет собой независимую от идентификации процедуру, которая имеет физических смысл достоверного определения факта превышения любым значением интенсивности $\lambda^q_{\text{п.к.а}}$ на предыдущем временном интервале $\tau_{\text{наб}}$ (отсчета параметра ($\lambda^1_{\text{п.к.а}}$)) над значением с каждого последующего отсчета ($\lambda^2_{\text{п.к.а}}$), на следующем временном интервале ($\tau_{\text{наб}}$ + 1), и осуществляется, например, для первого и второго временного интервала наблюдения в интересах оценки и прогнозирования уровня защищенности ОКИ, использующих ТИВ, в соответствии с выражением

$$\lambda^{1}_{\text{п.к.а}}(\tau_{\text{наб}}) \begin{matrix} > \\ < \end{matrix} \lambda^{2}_{\text{п.к.а}}(\tau_{\text{наб}}+1).$$

Сущность процедуры верификации состоит в выявлении тенденции (тренда) негативного изменения параметров внешних условий, тенденции медленного, плавного и, на первый взгляд, не вызывающего опасений роста интенсивности поступления (выявления) признаков компьютерной атаки в сторону угрожающего, граничного и даже потенциально катастрофичного уровня (состояния) защищенности ОКИ, использующих ТИВ.

С точки зрения практики в обоих случаях априорной оценки и прогнозирования, в случаях расчета и сравнения значений интенсивности поступления (выявления) признаков компьютерной атаки – как в рамках процедуры идентификации угрожающих, граничных и потенциально катастрофичных состояний защищенности, когда идентифицировано событие превышения

$$\lambda^{q}_{\text{п.к.а}}(\tau_{\text{наб}}+q) > \Lambda_{Q},$$

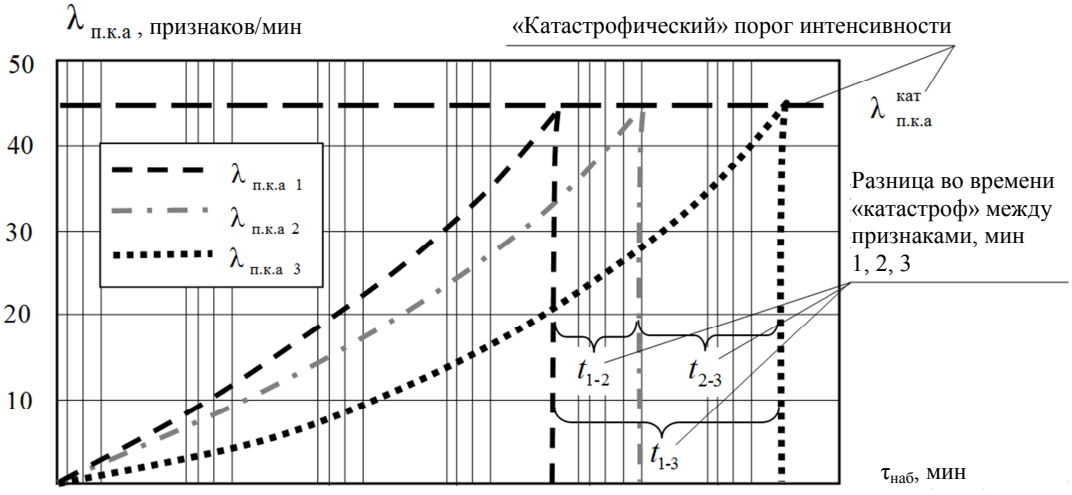
так и при осуществлении процедуры верификации, когда подтверждена тенденция (тренд) к изменению параметров внешних условий (есть медленный плавный рост интенсивности поступления признаков компьютерной атаки на данном шаге по сравнению с предыдущими) в сторону граничного и потенциально катастрофичного состояния защищенности ОКИ

$$\lambda^{1}_{\text{п.к.а}}(\tau_{\text{наб}}) < \lambda^{2}_{\text{п.к.а}}(\tau_{\text{наб}}+1),$$

пользователь (оператор, системный администратор), осуществляющий управление политикой безопасности ОКИ, использующих ТИВ, может и должен быть оповещен о возможном граничном и потенциально катастрофичном состоянии (уровне) защищенности объекта такого класса.

Результаты экспериментальных вычислений для примера оценки и прогнозирования состояния (уровня) защищенности с учетом интенсивности поступления (выявления) различных признаков компьютерных атак

В общем случае графическая интерпретация примера возможных результатов оценки и прогнозирования состояния (уровня) защищенности ОКИ, использующих ТИВ, для различных ситуаций, характеризуемых типом признака атаки, временем наблюдения, количеством временных отрезков наблюдения («глубиной прогнозирования») и различной интенсивностью поступления (выявления) признаков конкретного типа компьютерной атаки, выглядит так, как показано на рис.



Графическая интерпретация примера результатов оценки и прогнозирования состояния (уровня) защищенности ОКИ, использующих ТИВ, для различных ситуаций интенсивности признаков атак с использованием методов теории катастроф

Graphical interpretation of an example of the results of assessing and predicting the state (level) of security of CIO using ITT for various situations of the intensity of signs of attacks using the methods of disaster theory

Здесь, в качестве примера, интенсивность поступления (выявления) признаков конкретного типа компьютерной атаки $\lambda_{\text{п.к.а 1}}$ подразумевает, что речь идет о признаках агрессивного и несанкционированного сканирования потенциальным нарушителем портов компьютера или сервера, $\lambda_{\text{п.к.а 2}}$ – о призна-

ках, указывающих на резкое падение производительности компьютера, а $\lambda_{\text{п.к.а 3}}$ – о признаках компьютерной атаки, указывающих на интенсивность сбоев в учетных записях.

Интенсивность измеряется в количестве поступающих (выявленных) признаков конкретного типа компьютерной атаки за минуту (например, от 0 до 50 признаков в минуту), причем в качестве примера введен условный «катастрофический» порог интенсивности $\lambda_{\text{п.к.а}}^{\text{кат}}$, примерно равный 45 выявленным (поступившим) признакам в минуту, достигнув которого уровень защищенности «рушится». Временные интервалы прогнозирования ($\tau_{\text{наб}} + 1$), ($\tau_{\text{наб}} + 2$), ... и т. д., в качестве примера, условно взяты по 30 мин.

Графики иллюстрируют, что при плавных и медленных изменениях интенсивности поступления (выявления) признаков конкретного типа компьютерной атаки $\lambda_{\text{п.к.а 1}}$ – признаков агрессивного и несанкционированного сканирования потенциальным нарушителем портов компьютера или сервера – катастрофические последствия («обвал» уровня защищенности) наступают раньше, чем при иных, причем можно осуществить даже временной прогноз, – сравнив разницу во времени «катастроф» (между $t_{1\text{-}2}$, $t_{2\text{-}3}$ и $t_{1\text{-}3}$) для различных медленно изменяющихся признаков компьютерной атаки.

Таким образом, результаты примерных экспериментальных вычислений для рассмотренных, в качестве иллюстративного образца, условий показывают, что существует возможность с помощью математики теории катастроф осуществить оценку и прогнозирование уровня защищенности ОКИ, использующих ТИВ, для различных категорий потенциальных угроз инфраструктуре и отдельным элементам критических объектов такого класса.

Заключение

Рассмотрены базовые концептуальные аспекты, математические и методологические особенности применения методов теории катастроф (в части исследования бифуркаций), а также ключевые этапы реализации процедур идентификации и верификации уровня защищенности в рамках методов теории катастроф, применительно к различным ситуациям, характеризуемым типом признака угрозы защищенности (типом признака компьютерной атаки), временем наблюдения, количеством временных отрезков наблюдения – «глубиной прогнозирования» и различной интенсивностью поступления (выявления) признаков конкретного типа компьютерной атаки.

Предложенный подход позволяет повысить достоверность оценки и прогноза уровня защищенности подобных сложных критических объектов в интересах своевременного предупреждения об опасности и принятия мер для повышения их защиты в рамках принятой политики информационной безопасности. При этом трудоемкость процедур идентификации и верификации уровня защищенности в рамках методов теории катастроф, т. е. трудоемкость задачи идентификации и верификации граничного и потенциально угрожающего уровня (состояния) защищенности при плавно нарастающих негативных изменениях параметров внешних условий относительно невелика и связана в основном с затратами ресурсов на систематический пошаговый контроль, последовательное и методичное выявление и измерение потенциально угрожающих, граничных и экстремально-опасных состояний (уровней) защищенности.

Практическая новизна предложенного подхода, на наш взгляд, заключается в возможности предупреждения, заблаговременного оповещения пользователя (оператора, системного администратора) о возможном граничном и потенциально катастрофичном состоянии (уровне) защищенности объекта критической инфраструктуры такого класса.

Применение предложенного похода при оценке и прогнозировании уровня защищенности сложных информационно-технических объектов возможно как в рамках исследовательских работ, так и в системах автоматизированного мониторинга информационной безопасности любых инфраструктур сложных управляемых киберфизических систем как критического, так и некритического характера.

Направлением дальнейших исследований может быть разработка методов оценки и прогнозирования уровня защищенности, сочетающих методы теории катастроф (в частности, рассмотренные подходы к исследованию бифуркаций) и нечеткие множества, характеризующие нечетко-лингвистические парадигмы описания угроз.

Список источников

1. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Vector-based Dynamic Assessment of Cyber-Security of Critical Infrastructures // 2022 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) (25–28 Jan. 2022, St. Petersburg and Moscow, Russia). IEEE Xplore Digital Library, 2022. P. 277–282.

2. Lewis T. G. Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. NY: John Wiley & Sons Limited, 2019. 467 p.

3. Radvanovsky R. S., McDougall A. Critical Infrastructure. Homeland Security and Emergency Preparedness. Boca Raton: CRC Press, 2018. 344 p.

4. Верещагина Е. А., Капецкий И. О., Ярмонов А. С. Проблемы безопасности Интернета вещей: учеб. пособие. М.: Мир науки, 2021. 105 с.

5. Котенко И. В., Паращук И. Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2022. № 2. С. 33–40.

6. Kotenko I. V., Parashchuk I. B., Desnitsky V. A. Determination of the Transition Probability Matrix for an IoT Fuzzy Security Model // 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) (28–30 November 2023, Bali, Indonesia). IEEE Xplore Digital Library, Browse Conferences, 2023. P. 40–44.

7. Котенко И. В., Саенко И. Б., Паращук И. Б. Обнаружение и противодействие сетевым атакам на основе анализа трафика: основные направления исследований // Перспективные направления развития отечественных информационных технологий: материалы VI Межрегион. науч.-практ. конф. (Севастополь, 22–26 сентября 2020 г.). Севастополь: Изд-во СевГУ, 2020. Т. 1. С. 187–188.

8. Ховард Р. Кибербезопасность: главные принципы. СПб.: Питер, 2024. 320 с.

9. Kamara M. K. Securing Critical Infrastructures. Bloomington: Xlibris, 2020. 385 p.

10. Kyriakides E., Polycarpou M. Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems. Berlin: Springer, 2015. 359 p.

11. Маничев С. А., Лепехин Н. Н. Проактивный менеджмент безопасности и проактивное поведение персонала как ресурсы инжиниринга устойчивости // Вестн. Санкт-Петерб. ун-та. Психология. 2020. Т. 10. Вып. 1. С. 33–45.

12. Bailey B., Doleman R. Proactive Security Protection of Critical Infrastructure: A Process Driven Methodology. NY: Independently published, 2013. 28 p.

13. Haiquan L., Haibo D., Ping S., Pei L., Baoyun W. Proactive eavesdropping in UAV-aided mobile relay systems // EURASIP Journal on Wireless Communications and Networking. 2020. V. 2020. N. 48. P. 1993–1997.

14. Kermabon-Bobinnec H., Gholipourchoubeh M., Bagheri S., Majumdar S., Jarraya Y., Pourzandi M., Wang L. Proactive Security Policy Enforcement for Containers (ProSPEC) // Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy (CODASPY ’22) (April 24-27, 2022, Baltimore, MD, USA). NY: ACM, 2022. P. 511–515.

15. Арнольд В. И. Теория катастроф. М.: Ленанд, 2025. 136 с.

16. Poston T., Stewart I. Catastrophe Theory and Its Applications (Dover Books on Mathematics). NY: Dover Publications, 2012. 512 p.

17. Saunders P. T. An Introduction to Catastrophe Theory. Cambridge: Cambridge University Press, 2013. 201 p.

References

1. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Vector-based Dynamic Assessment of Cyber-Security of Critical Infrastructures. *2022 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) (25-28 Jan. 2022, St. Petersburg and Moscow, Russia)*. IEEE Xplore Digital Library, 2022. Pp. 277-282.

2. Lewis T. G. *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation*. New York, John Wiley & Sons Limited, 2019. 467 p.

3. Radvanovsky R. S., McDougall A. *Critical Infrastructure. Homeland Security and Emergency Preparedness.* Boca Raton, CRC Press, 2018. 344 p.

4. Vereshchagina E. A., Kapetskii I. O., Iarmonov A. S. *Problemy bezopasnosti Interneta veshchei: uchebnoe posobie* [Internet of Things Security Issues: A study guide]. Moscow, Mir nauki Publ., 2021. 105 p.

5. Kotenko I. V., Parashchuk I. B. Informatsionnye i telekommunikatsionnye resursy kriticheski vazhnykh infrastruktur: osobennosti interval'nogo analiza zashchishchennosti [Information and telecommunication resources of critical infrastructures: features of interval security analysis]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2022, no. 2, pp. 33-40.

6. Kotenko I. V., Parashchuk I. B., Desnitsky V. A. Determination of the Transition Probability Matrix for an IoT Fuzzy Security Model. *2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) (28–30 November 2023, Bali, Indonesia)*. IEEE Xplore Digital Library, Browse Conferences, 2023. Pp. 40-44.

7. Kotenko I. V., Saenko I. B., Parashchuk I. B. Obnaruzhenie i protivodeistvie setevym atakam na osnove analiza trafika: osnovnye napravleniia issledovanii [Detecting and countering network attacks based on traffic analysis: main research directions]. *Perspektivnye napravleniia razvitiia otechestvennykh informatsionnykh tekhnologii: materialy VI Mezhregional'noi nauchno-prakticheskoi konferentsii (Sevastopol', 22–26 sentiabria 2020 g.).* Sevastopol', Izd-vo SevGU, 2020. Vol. 1. Pp. 187-188.

8. Khovard R. *Kiberbezopasnost': glavnye printsipy* [Cybersecurity: the main principles]. Saint Petersburg, Piter Publ., 2024. 320 p.

9. Kamara M. K. *Securing Critical Infrastructures*. Bloomington, Xlibris, 2020. 385 p.

10. Kyriakides E., Polycarpou M. *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*. Berlin, Springer, 2015. 359 p.

11. Manichev S. A., Lepekhin N. N. Proaktivnyi menedzhment bezopasnosti i proaktivnoe povedenie personala kak resursy inzhiniringa ustoichivosti [Proactive safety management and proactive personnel behavior as sustainability engineering resources]. *Vestnik Sankt-Peterburgskogo universiteta. Psikhologiia*, 2020, vol. 10, iss. 1, pp. 33-45.

12. Bailey B., Doleman R. *Proactive Security Protection of Critical Infrastructure: A Process Driven Methodology.* New York, Independently published, 2013. 28 p.

13. Haiquan L., Haibo D., Ping S., Pei L., Baoyun W. Proactive eavesdropping in UAV-aided mobile relay systems. *EURASIP Journal on Wireless Communications and Networking*, 2020, vol. 2020, no. 48, pp. 1993-1997.

14. Kermabon-Bobinnec H., Gholipourchoubeh M., Bagheri S., Majumdar S., Jarraya Y., Pourzandi M., Wang L. Proactive Security Policy Enforcement for Containers (ProSPEC). *Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy (CODASPY '22) (April 24-27, 2022, Baltimore, MD, USA)*. New York, ACM, 2022. Pp. 511-515.

15. Arnol'd V. I. *Teoriia katastrof* [The theory of catastrophes]. Moscow, Lenand Publ., 2025. 136 p.

16. Poston T., Stewart I. *Catastrophe Theory and Its Applications (Dover Books on Mathematics)*. New York, Dover Publications, 2012. 512 p.

17. Saunders P. T. *An Introduction to Catastrophe Theory*. Cambridge, Cambridge University Press, 2013. 201 p.

Статья поступила в редакцию 20.03.2025; одобрена после рецензирования 28.04.2025; принята к публикации 22.08.2025
The article was submitted 20.03.2025; approved after reviewing 28.04.2025; accepted for publication 22.08.2025

Информация об авторах / Information about the authors

Игорь Витальевич Котенко – доктор технических наук, профессор; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности; Санкт-Петербургский институт информатики и автоматизации Российской академии наук; ivkote@comsec.spb.ru

Igor V. Kotenko – Doctor of Technical Sciences, Professor; St. Petersburg Federal Research Center of the Russian Academy of Sciences; Chief Scientist and Head of the Laboratory of Computer Security Problems; St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; ivkote@comsec.spb.ru

Дмитрий Сергеевич Левшун – кандидат технических наук, доцент; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; доктор философии компьютерных наук; ведущий научный сотрудник лаборатории проблем компьютерной безопасности; Санкт-Петербургский институт информатики и автоматизации Российской академии наук; dmitry.levshun@gmail.com

Dmitry S. Levshun – Candidate of Technical Sciences, Assistant Professor; St. Petersburg Federal ResearchCenter of the Russian Academy of Sciences; PhD in Computer Science; Leading Researcher of the Laboratory of Computer Security Problems; St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; dmitry.levshun@gmail.com

Игорь Борисович Паращук – доктор технических наук, профессор; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; ведущий научный сотрудник лаборатории проблем компьютерной безопасности; Санкт-Петербургский институт информатики и автоматизации Российской академии наук; shchuk@rambler.ru

Igor B. Parashchuk – Doctor of Technical Sciences, Professor; St. Petersburg Federal Research Center of the Russian Academy of Sciences; Leading Researcher of the Laboratory of Computer Security Problems; St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; shchuk@rambler.ru