ISSN 2413–9599 (Print)
ISSN 2541–870X (Online)

www.radioprom.org

DOI: 10.21778/2413-9599-2018-28-4-59-67
УДК 004.056

Критическая информационная инфраструктура: оценка устойчивости функционирования

В.А. Минаев[1], И.Д. Королев[2], Е.В. Зеленцова[1], Р.И. Захарченко[2]

[1] Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия
[2] Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, Краснодар, Россия

В статье рассматривается подход к оценке критической информационной инфраструктуры, циркулирующей в информационной системе в условиях противоборства. Новизна работы заключается в использовании перспективного метода, который позволяет оценивать сложные технические системы, обладающие высокой степенью критичности и неопределенностью описания. В качестве оценки способности реализации целевой функции критической информационной инфраструктуры в каждый момент времени предложено значение интегрального критерия. На основании этого метода появилась возможность повысить качество обоснования новых способов противоборства в информационном пространстве. В статье решены задачи устойчивости информационной системы. Рассмотрены ее основные компоненты и свойства управления, определяющие устойчивость функционирования системы в целом. Предложена классификация систем критической информационной инфраструктуры. Дано формальное определение показателя киберустойчивости и приведены методика и алгоритм его расчета. Практическая значимость состоит в том, что новый метод оценки может быть использован для повышения эффективности управления критической информационной инфраструктурой.

Ключевые слова: кибернетическое пространство, информационное противоборство, компьютерная атака, киберустойчивость, деструктивное информационное воздействие, критическая информационная инфраструктура

Для цитирования:
Критическая информационная инфраструктура: оценка устойчивости функционирования / В.А. Минаев, И.Д. Королев, Е.В. Зеленцова, Р.И. Захарченко // Радиопромышленность. 2018. Т. 28, № 4. С. 59–67. DOI: 10.21778/2413-9599-2018-28-4-59-67

Critical information infrastructure: sustainability assessment

V.A. Minaev[1], I.D. Korolev[2], E.V. Zelentzova[1], R.I. Zakharchenko[2]

[1] Bauman Moscow State Technical University, Moscow, Russia
[2] Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia

The paper considers the approach to the assessment of critical information infrastructure circulating in the information system in terms of confrontation. The novelty of the study is a promising method allowing assessment of complex technical systems with a high degree of criticality and uncertainty of description. The value of the integral criterion is proposed as an assessment of the ability to implement the objective function of critical information infrastructure at each time point. Based on this method, it became possible to improve the quality of substantiation of new ways of confrontation in the information space. The paper addresses the problem of information system stability. Its main components and management properties that determine the stability of the system functioning as a whole are considered. A classification of critical information infrastructure systems is proposed. A formal definition of the cyber resistance index, as well as method and algorithm for its calculation, are given. The practical significance is that the new method of assessment can be used to improve the efficiency of critical information infrastructure management.

Keywords: cyberspace, informational confrontation, cyber attacks, cyber resistance, destructive information influence, critical information infrastructure

For citation:
Minaev V.A., Korolev I.D., Zelentzova E.V., Zakharchenko R.I. Critical information infrastructure: sustainability assessment. Radiopromyshlennost, 2018, vol. 28, no. 4, pp. 59–67. (In Russian). DOI: 10.21778/2413-9599-2018-28-4-59-67

Введение

Значительное повышение уровня автоматизированных комплексов управления, информационных технологий и информационных систем, создание единого информационного пространства предопределили возникновение и развитие принципиально нового объекта планетарного масштаба – киберпространства [1]. Феномен наличия и успешного функционирования данного объекта при отсутствии его достаточно развитой теории не соответствует практике создания сложных искусственных систем [2–4]. При этом речь идет об искусственных воздействиях и искусственной среде его существования, порождающих в свою очередь новые де-факто сложившиеся, но юридически не закрепленные в Российской Федерации термины и их трактовку. Хотя уже появились работы по исследованию терминологии в данной области [5, 6].

Доступность через киберпространство критической информационной инфраструктуры (КИИ) ставит обеспечение национальной безопасности в зависимость от степени ее защищенности. Под КИИ будем понимать множество автоматизированных систем управления, при помощи которых обеспечивается взаимодействие информационно-телекоммуникационных сетей, решающих задачи государственного управления, вопросы обороноспособности, проблемы безопасности и правопорядка, нарушение или прекращение функционирования которых приводит к наступлению тяжелых последствий. Защищенность КИИ напрямую зависит от владения соответствующими структурами новым видом оружия (кибероружием, отвечающим среде ее функционирования), от степени эффективности, методов использования и средств защиты этого оружия. Все перечисленное создает необходимые предпосылки для возникновения и осуществления действенного противоборства в киберпространстве.

Кибернетическое оружие, вырабатывающее деструктивные информационные воздействия, не является оружием в классическом смысле, т.к. не осуществляет физическое поражение объекта атаки, а переводит его информационную систему и автоматизированную систему управления в кризисный режим функционирования.

Процесс противодействия двух и более сторон представляет собой кибернетическое противоборство, реализуемое при использовании совместного общего ресурса – глобального информационного пространства. Управление им определяют как целевое воздействие двух и более подсистем управления, пытающихся расширить друг на друга эти управляющие воздействия (рис. 1).

В результате противоборства в киберпространстве нарушается функционирование объектов КИИ, и это может привести к нежелательным эффектам. Например, к временной потере управления объектом или физическому разрушению объектов КИИ.

Эта проблема приобретает значительную актуальность при решении задач обеспечения безопасности объектов КИИ, имеющих особо важное значение (химические заводы, атомные электростанции и т.п.), при разрушении которых может быть нанесен фатальный ущерб прилегающим объектам и территориям, а также обслуживающему персоналу и населению. Так, по оценке экспертов [7], эффект целевого применения кибернетического оружия против информационной системы сравним с эффектом применения оружия массового поражения.

Отсюда следует, что действия объектов КИИ в кибернетическом пространстве создают новые уязвимости и угрозы и требуют разработки новых инструментов, обеспечивающих безопасность КИИ, которые бы гарантировали стабильную работоспособность в условиях компьютерных атак любой интенсивности [5].

Проблема устойчивости критической информационной инфраструктуры

Как же оценить устойчивость функционирования такой сложной социотехнической системы, как КИИ?

Анализ научных источников и литературы, изложенный в работе [5], по организации безопасности КИИ, обеспечению надежности и устойчивого функционирования автоматизированной системы управления объектов КИИ показал, что в них не рассмотрены следующие вопросы, связанные с разработкой моделей, методов и методик [4]:

- оценка состояния объектов КИИ;
- формирование признакового пространства функционирования КИИ;
- создание и ведение единой распределенной базы данных с оперативной аналитической обработкой данных [4];
- адаптивное управление КИИ, учитывающих текущее и прогнозируемое состояние объектов КИИ в условиях деструктивных информационных воздействий [4].

Кроме того, разработан, но является малоэффективным научно-методический аппарат проектирования автоматической системы сбора данных. Необходимо решить задачу приведения информации к единому виду, определяющей состояние КИИ в условиях деструктивных информационных воздействий.

Из сказанного следует, что существует потребность в разработке способов проектирования системы оценки функциональной устойчивости КИИ в условиях информационного противоборства. При этом надо отметить, что представленная на рис. 1 упрощенная модель позволяет сформулировать и описать важнейшие качества и свойства управления, определяющие киберустойчивость [5, 8, 9] (рис. 2).

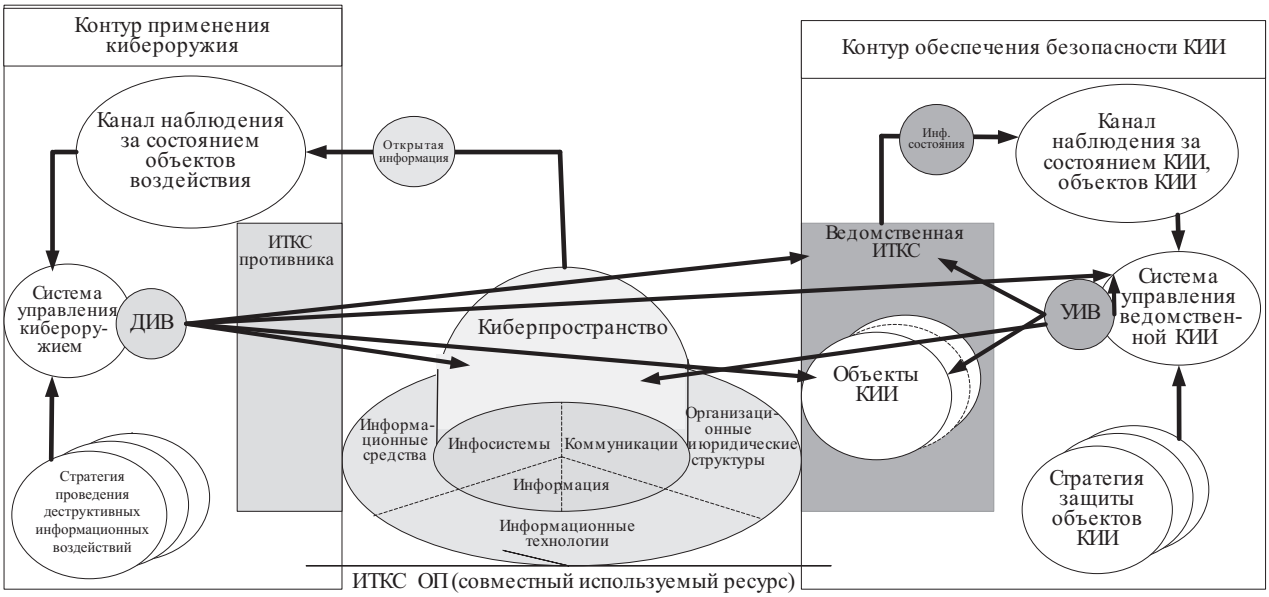

Рисунок 1. Модель информационного противодействия в кибернетическом пространстве: ИТКС – информационно-телекоммуникационные системы; УИВ – уязвимости информационных воздействий; ДИВ – деструктивные информационные воздействия
Figure 1. The model of information confrontation in cyberspace: ИТКС – information and telecommunication systems; УИВ – vulnerabilities of information impacts; ДИВ – destructive information influences

На процесс управления КИИ кибернетическое противоборство накладывает дополнительные требования по обеспечению устойчивого функционирования КИИ. Устойчивость при этом является интегральным свойством, неотъемлемо связанным со средой функционирования.

Способы управления киберустойчивостью

С устойчивостью в техно- и инфосфере все более или менее определено, чего не скажешь про устойчивость в киберпространстве (киберустойчивость). Здесь возникает ряд вопросов, связанных с виртуальностью указанной среды. Причем процессы, происходящие в ней, оказывают прямые или косвенные воздействия, сказывающиеся на устойчивости функционирования КИИ в техно- и инфосфере.

Анализ рис. 2 показывает, что киберустойчивость является интегральным показателем и определяется киберживучестью, киберпомехоустойчивостью и кибернадежностью, которые отражают возможность выполнять свои задачи в сложной, резко изменяющейся обстановке, системе управления КИИ в условиях информационных деструктивных воздействий.

Объекты критической информационной инфраструктуры и их классификация

Существует многообразие объектов КИИ. Для последующего исследования необходимо их классифицировать (рис. 3). Ниже приведем

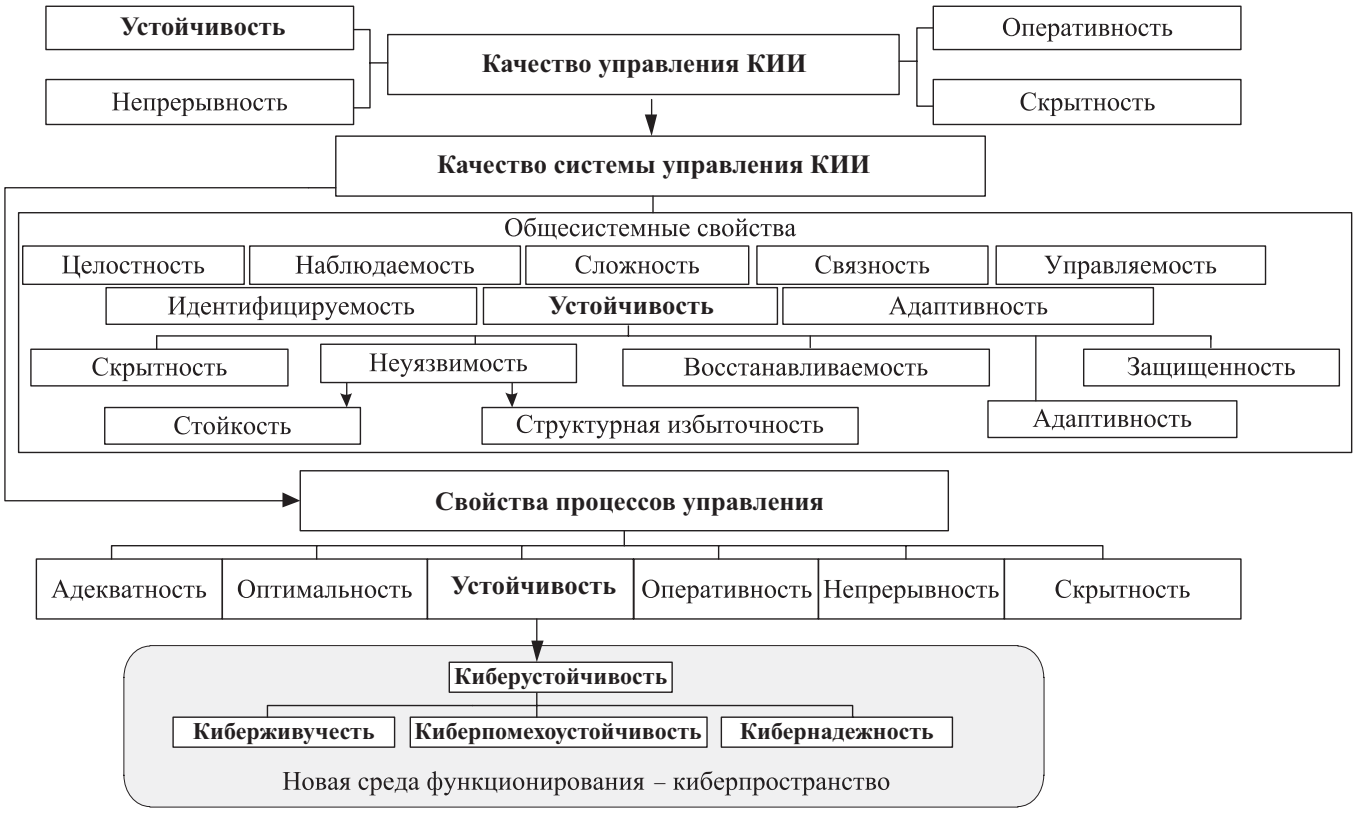

Рисунок 2. Качества и свойства управления, определяющие киберустойчивость
Figure 2. Quality and management properties that determine a cyber resistance

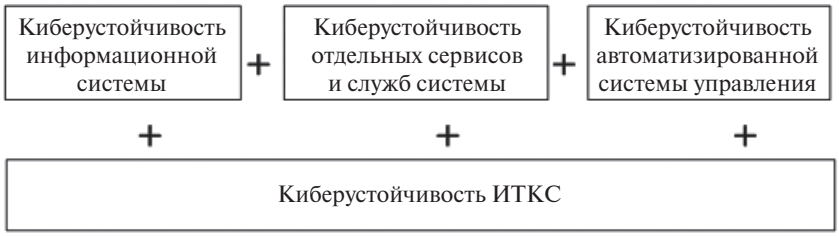

Рисунок 3. Слагаемые обеспечения киберустойчивости КИИ
Figure 3. Components for ensuring the cyber stability of critical infrastructure

классификацию по признакам, которые оказывают негативное воздействие на функционирование киберустойчивости:

1. По организационной структуре:
   - Однозвенный объект КИИ (состоит из одного звена) обладает всеми необходимыми возможностями для выполнения единичной целевой функции (самостоятельный базовый сегмент). Отдельные комплексы средств автоматизации могут служить примером однозвенной структуры.
   - Многозвенный объект КИИ (состоит из многих звеньев) представляет собой структурное последовательное соединение в единую систему нескольких однозвенных объектов КИИ для достижения единой целевой функции.
2. По функциональному единству:
   - Однородные многозвенные объекты КИИ – это объекты, образованные из последовательного соединения однозвенных объектов КИИ в единую систему, имеющих единую целевую функцию, для выполнения единой целевой функции.
   - Неоднородные многозвенные объекты КИИ – это объекты, образованные из последовательного соединения однозвенных объектов КИИ и выполняющие различные целевые функции, например информационные системы, системы обработки данных, телекоммуникационная сеть и т.д.

Приведенная классификация помогает оценить киберустойчивость как совокупность взаимосвязанных сложных организационных систем (учитывая коэффициент связанности) однозвенных объектов КИИ (принимая во внимание индивидуальный вклад в выполнение системой целевой функции).

При этом под киберустойчивостью однозвенного объекта КИИ будем понимать способность его системы управления выполнять свои функции при всех видах деструктивных информационных воздействий.

Показатель киберустойчивости

Для однозвенного объекта КИИ обобщенный показатель киберустойчивости $К_{окии^{уо}}$ имеет следующий вид:

$$К_{окии^{уо}} = К_{окии^{жив}} К_{окии^{пом}} К_{окии^{над}}, \quad (1)$$

где $К_{окии^{жив}}$ – киберживучесть КИИ, т.е. вероятность сохранения у объектов КИИ работоспособности при выходе из строя технических средств обработки информации, отражает вклад каждого элемента КИИ однозвенного объекта при выполнении целевой функции; $К_{окии^{пом}} = (1 - Р_{ПКА}) \times (1 - Р_{ПЦКА})$ – киберпомехоустойчивость однозвенного объекта КИИ, понимаемая как вероятность реализации целевой функции объекта КИИ в условиях соблюдения «общих» и деструктивных информационных воздействий с заданным качеством; $Р_{ПКА}$ и $Р_{ПЦКА}$ – вероятности разрушения технических средств обработки информации, которые входят в объект КИИ, направленными деструктивными информационными воздействиями; $К_{окии^{над}}$ – кибернадежность КИИ однозвенного объекта, характеризующая вероятность условий выполнения целевой функции объекта КИИ на определенном временном интервале при появлени разнообразных событий ($i = 1, ..., N$) – ошибок в программах, непредумышленных неправильных действий технического персонала, сбоев техники и ошибочных действий должностных лиц объекта КИИ, определяемая как

$$К_{окии^{над}} = \Pi_{i=1}^{N} К_{окии^{над_i}} (1 - P_i), \quad (2)$$

где P_i – вероятность i-го события ($i = 1, ..., N$).

На этапе проектирования к объектам КИИ предъявляют серьезные требования по технической надежности. Определяют перечень спецмер по увеличению эффективности нейтрализации отказов программных и технических средств при обработке информации. Например, это может происходить за счет кластеризации серверов или резервирования отдельных компонентов технических средств обработки информации (ТСОИ), обладающих низкой надежностью. Исходя из этого, когда определяют киберустойчивость КИИ в условиях деструктивных информационных воздействий при своевременном и высококачественном техническом обслуживании, вероятность технических отказов ТСОИ можно считать незначительной. При этом кибернадежность КИИ однозвенного объекта $К_{окии^{уо}}$ можно найти из формулы

$$К_{окии^{уо}} = К_{окии^{жив}} К_{окии^{пом}}. \quad (3)$$

При отказе звеньев КИИ, вызванном независимыми событиями, в условиях деструктивных информационных воздействий киберустойчивость КИИ многозвенного объекта $К_{окии^{ум}}$ определяют по формуле

$$K_{окии^{ум}}(N) = \Pi_{i=1}^{N} K_{окии^{уо_i}}, \quad (4)$$

где $К_{окии^{уо_i}}$ – обобщенный показатель киберустойчивости i-го однозвенного объекта.

В других случаях киберустойчивость КИИ многозвенного объекта рассчитывают как N-мерную вероятность совместного одновременного сохранения работоспособности N звеньев, которые составляют данный объект:

$$К_{окии^{ум}}(N) = P\{К_{окии^{уо1}} \geq К_{окии^{уодоп}}, ..., К_{окии^{уоN}} \geq К_{окии^{уодоп}}\}, \quad (5)$$

где для каждого i-го события ($i = 1, ..., N$) введены допустимые значения вероятностей $K_{ОКИИ}^{УОдоп}$.

Из выражений (3) и (4) следует, что основой для определения киберустойчивости объектов КИИ является расчет показателей киберпомехоустойчивости и киберживучести индивидуальных звеньев объекта КИИ. Определяющим свойством выполнения объектом КИИ целевой функции является киберживучесть, а ее составной частью выступает киберпомехоустойчивость.

Киберживучесть объектов критической информационной инфраструктуры

Свойства, которые характеризуют киберживучесть объекта КИИ при осуществлении деструктивных информационных воздействий, проявляются только после того, как КИИ подверглась атаке, в связи с этим мера живучести определяется условной вероятностью сохранения работоспособности при условии, что система получила локальное повреждение [10].

Под показателем киберживучести однозвенного объекта $K_{ОКИИ}^{жив}$ понимаем условную вероятность невыхода его конечного состояния за границы заданной области безопасных состояний S^I пространства S в случае деструктивных информационных воздействий:

$$K_{ОКИИ}^{жив} = P\left[\left(\|S - s_0\| < S^1\right)/\Omega\right], \quad (6)$$

где s_0 – область пространства, подвергшаяся деструктивным воздействиям; Ω – деструктивное информационное воздействие.

Исходя из определения структурной уязвимости системы [11, 12], под которой понимается вероятность выхода конечного состояния системы из заданной безопасной области $S^I - V_S$, справедливо соотношение

$$K_{ОКИИ}^{жив} = 1 - V_s, \quad (7)$$

а в конкретной точке на исследуемом временном интервале

$$K_{ОКИИ}^{жив}(t) = 1 - V_s(t). \quad (8)$$

Киберживучесть КИИ однозвенного объекта будем определять оценкой критерия по соотношению

$$K_{ОКИИ}^{тек\ жив}(t) \geq K_{ОКИИ}^{тр\ жив}(t). \quad (9)$$

Здесь $K_{ОКИИ}^{тек\ жив}(t)$ – текущий уровень живучести однозвенного объекта КИИ; $K_{ОКИИ}^{тр\ жив}(t)$ – требуемый уровень живучести однозвенного объекта КИИ в условиях деструктивных информационных воздействий.

Способность объекта КИИ выполнять целевую функцию $W_б$ в условиях деструктивных информационных воздействий определим, используя выражения (5), (7), (9):

$$W_б = \begin{cases} K_{ОКИИ}^{тек\ жив}(t) > 0{,}9 - \text{объект полностью выполнен;} \\ 0{,}9 \leq K_{ОКИИ}^{тек\ жив}(t) < 0{,}7 - \text{объект в целом выполнен;} \\ 0{,}7 \leq K_{ОКИИ}^{тек\ жив}(t) < 0{,}5 - \text{объект ограниченно выполнен;} \\ 0{,}5 \leq K_{ОКИИ}^{тек\ жив}(t) < 0{,}3 - \text{объект не выполнен, подлежит восстановлению;} \\ K_{ОКИИ}^{тек\ жив}(t) \leq 0{,}3 - \text{объект не подлежит восстановлению.} \end{cases} \quad (10)$$

Общий коэффициент живучести $K_{ОКИИN}^{жив}$ (5), (6), (8), (10) определим исходя из введеных следующих уровней киберживучести:

$$K_{ОКИИN}^{жив}(t) = \begin{cases} K_{ОКИИ}^{тек\ жив}(t) - K_{ОКИИ}^{тр\ жив}(t) > 0 - \text{оптимальный уровень;} \\ K_{ОКИИ}^{тек\ жив}(t) - K_{ОКИИ}^{тр\ жив}(t) = 0 - \text{допустимый уровень;} \\ K_{ОКИИ}^{тек\ жив}(t) - K_{ОКИИ}^{тр\ жив}(t) < 0 - \text{критический уровень;} \\ K_{ОКИИ}^{тек\ жив}(t) = 0 - \text{закритический уровень (нулевой).} \end{cases} \quad (11)$$

Методика оценки киберустойчивости

Педлагаемая методика оценки киберустойчивости разбита на три этапа.

1. Оценка киберустойчивости каждого объекта КИИ отдельно.
   1.1. Выполнить оценку КИИ однозвенного объекта:
   - рассчитать киберпомехоустойчивость, т.е. вероятность выхода из строя i-го ТСОИ в условиях деструктивных информационных воздействий;
   - определить коэффициент связанности i-го ТСОИ и его вклад в целевую функцию объекта КИИ;
   - оценить киберживучесть, т.е. предел состояний КИИ однозвенного объекта.

   1.2. Выполнить оценку КИИ многозвенного объекта.
   - рассчитать киберпомехоустойчивость, т.е. вероятность выхода из строя j-го однозвенного объекта КИИ в условиях деструктивных информационных воздействий;
   - определить коэффициент связанности j-го КИИ однозвенного объекта и его вклад в целевую функцию КИИ многозвенного объекта;

- дать оценку киберживучести, т.е. предела состояний КИИ многозвенного объекта.

2. Оценка киберустойчивости взаимодействующих объектов КИИ:
   - рассчитать киберпомехоустойчивость, т.е. вероятность отказа n-го КИИ многозвенного объекта в условиях деструктивных информационных воздействий;
   - определить коэффициент связанности n-го КИИ многозвенного объекта и его вклад в целевую функцию КИИ многозвенного объекта;
   - дать оценку киберживучести.
3. Оценка киберустойчивости КИИ определяется через сумму значений устойчивости ее элементов с учетом коэффициента связанности, включающая оценку киберживучести КИИ в динамике при выполнении ею своих функций.

Реализация в виде блок-схемы методики оценки устойчивости функционирования КИИ приведена на рис. 4.

В рамках реализации подхода к оценке устойчивости функционирования объектов КИИ, которые действуют в киберпространстве, рекомендуется

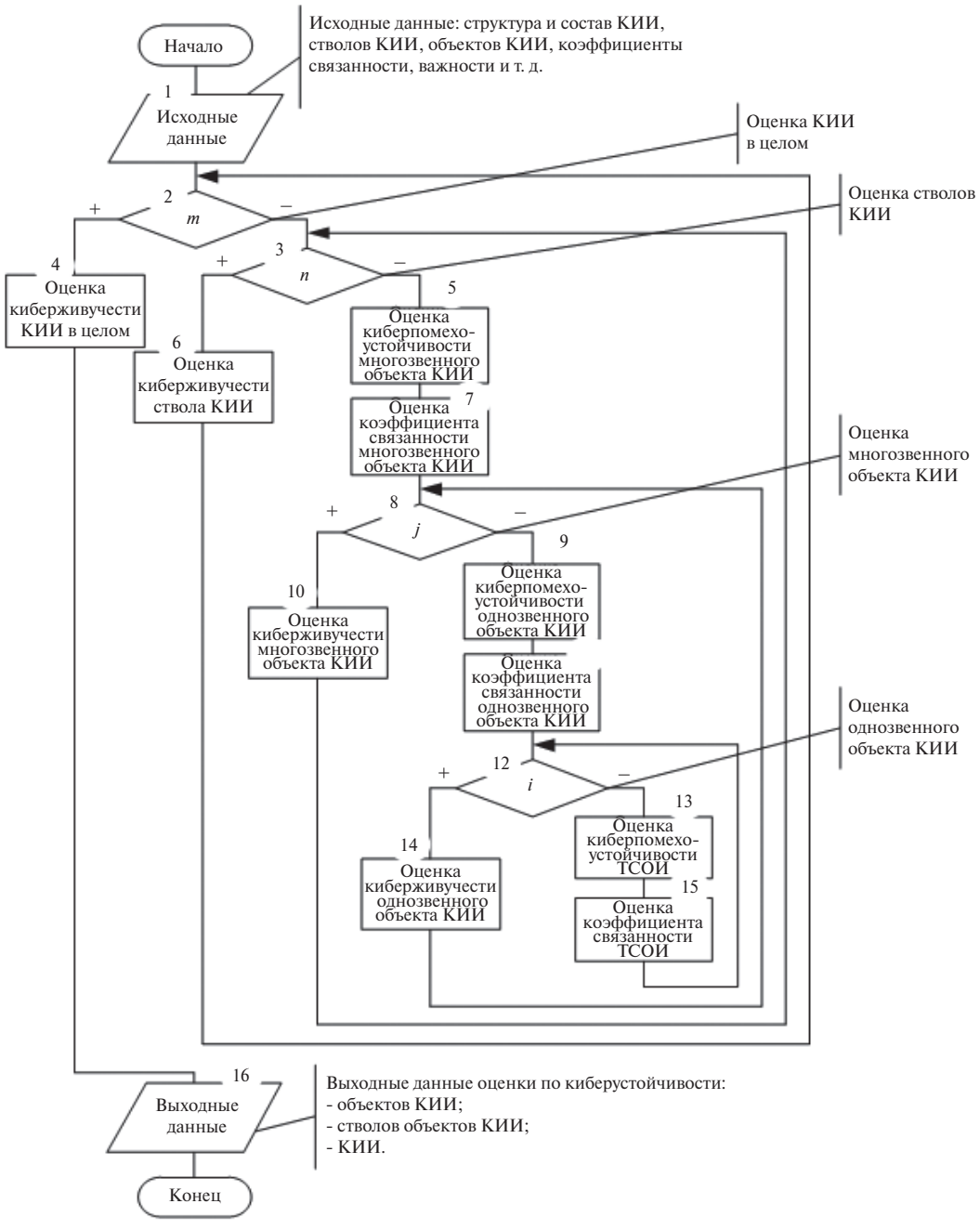

Рисунок 4. Блок-схема способа оценки устойчивости функционирования КИИ
Figure 4. Flow diagram of the method for assessing the sustainability of the critical information infrastructure functioning

расширить интегральные свойства устойчивости за счет реализации нового вида кибероружия, нейтрализирующего появление новых угроз и уязвимостей для объектов и в целом для КИИ. Предложенный способ декомпозиция КИИ позволяет оценить способность КИИ выполнять целевые функции с учетом их коэффициентов связанности и степени важности, выполняемых функций.

В соответствии с разработанной схемой отнесения класса состояния объекта к уровню качества, полученный результат (рис. 4) позволяет однозначно дать оценку устойчивости функционирования КИИ.

Выводы

1. Доступность КИИ ставит национальную безопасность в зависимость от степени ее защищенности. Защищенность при этом напрямую зависит от степени владения соответствующими структурами новым видом оружия – кибероружием, создающим необходимые предпосылки для возникновения и осуществления эффективного противоборства в киберпространстве.
2. Реализация функций объектов КИИ в кибернетическом пространстве создает новые уязвимости и угрозы, требуя создания современных инструментов, обеспечивающих безопасность КИИ, т.е. защищенность, обеспечивающая устойчивое функционирование КИИ в условиях компьютерных атак любой интенсивности.
3. Объекты КИИ целесообразно классифицировать по признакам, оказывающим влияние на обеспечение киберустойчивости функционирования: по организационной структуре – однозвенные и многозвенные; по функциональному единству – однородные многозвенные и неоднородные многозвенные.
4. Обобщенный показатель киберустойчивости включает показатели киберживучести, киберпомехоустойчивости и кибернадежности КИИ.
5. Методика оценки киберустойчивости представляется тремя последовательными этапами:
   - оценка киберустойчивости каждого отдельно действующего объекта КИИ;
   - оценка киберустойчивости объектов КИИ, действующих взаимно;
   - оценка киберустойчивости КИИ через сумму устойчивости ее элементов с учетом коэффициента связанности, включая оценку киберживучести КИИ в динамике при выполнении ею своих функций.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А.* Управление качеством информационных услуг. СПб.: Изд-во Политехнического университета, 2017. 454 с.
2. Глобальная безопасность в цифровую эпоху: стратагемы для России / под ред. А.И. Смирнова. М.: ВНИИгеосистем, 2014. 394 с.
3. *Бедриц А.В.* Информационная война: концепции и их реализация в США. М.: РИСИ, 2008. 187 с.
4. *Захарченко Р.И., Королев И.Д.* Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10, № 2. С. 52–61. DOI: 10.24411/2409-5419-2018-10041.
5. *Макаренко С.И., Чукляев И.И.* Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1(2). С. 13–21.
6. *Развитие* методологических основ информатики и информационной безопасности систем: депонированная рукопись № 1165-В2004. Дата депонирования: 07.07.2004 / А.П. Фисун, А.Г. Касилов, В.Е. Фисенко, В.А. Минаев, В.В. Афанасьев, В.В. Митяев, Р.А. Фисун, К.А. Джевага, С.А. Кожухов. М.: ВИНИТИ, 2004. 253 с.
7. *Grechishnikov E., Lybimov V., Komolov D.* Influence of the stages of operation of communication facilities on the model of variation of reliability. Telecommunications and Radio Engineering, 2010, vol. 69, iss. 3, pp. 247–256.
8. *Новиков Д.А.* Теория управления организационными системами. М.: МПСИ, 2005. 584 с.
9. Киберустойчивость информационно-телекоммуникационной сети: монография / М.А. Коцыняк, И.А. Кулешов, М.А. Кудрявцев, О.С. Лаута. СПб.: Бостон-спектр, 2015. 150 с.
10. *Казаков В.И.* Основы теории топогеодезического обеспечения боевых действий войск. М.: ВИА, 1977. С. 32–36.
11. *Махутов Н.А., Резников Д.О., Петров П.В.* Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47–66.
12. *Минаев В. А, Королев И.Д., Мухортов В.В.* Марковские модели защиты информационных систем беспилотных робототехнических объектов // Технологии техносферной безопасности. 2016. Вып. 6 (70). [Электронный ресурс]. URL: http://agps-2006.narod.ru/ttb/2016-6/17-06-16.ttb.pdf (дата обращения: 15.10.2018).

REFERENCES

1. Starodubtsev Yu. I., Begaev A.N., Davlyatova M.A. *Upravlenie kachestvom informatsionnykh uslug* [Information services quality management]. St. Petersburg, Izdatelstvo Politekhnicheskogo universiteta Publ., 2017. 454 p. (In Russian).
2. Smirnov A.I. (ed.). *Globalnaya bezopasnost v cifrovuyu ehpohu: stratagemy dlya Rossii* [Global security in the digital era: stratagems for Russia]. Moscow, VNIIgeosistem Publ., 2014. 394 p. (In Russian).
3. Bedrits A.V. Informacionnaya vojna: koncepcii i ih realizaciya v SShA [Information warfare: concepts and their implementation in the United States]. Moscow, RISI Publ., 2008, 187 p. (In Russian).

4. Zakharchenko R. I., Korolev I. D. Methods of assessing the sustainability of the objects of critical information infrastructure functioning in cyberspace. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli,* 2018, vol. 10, no. 2. pp. 52–61. (In Russian). DOI: 10.24411/2409-5419-2018-10041.
5. Makarenko S. I., CHuklyaev I. I. The terminological basis of the informational conflict area. *Voprosy kiberbezopasnosti,* 2014, no. 1 (2), pp. 13–21. (In Russian).
6. Fisun A. P., Kasilov A. G., Fisenko V. E., Minaev V. A., Afanasev V. V., Mityaev V. V., Fisun R. A., Dzhevaga K. A., Kozhuhov S. A. *Razvitie metodologicheskih osnov informatiki i informacionnoj bezopasnosti sistem* [Development of methodological foundations of computer science and information systems security]: deposited script no. 1165-V2004. Date of deposit: 07.07.2004. Moscow, VINITI Publ., 2004. 253 p. (In Russian).
7. Grechishnikov E., Lybimov V., Komolov D. Influence of the stages of operation of communication facilities on the model of variation of reliability. *Telecommunications and Radio Engineering,* 2010, vol. 69, iss. 3, pp. 247–256.
8. Novikov D. A. Teoriya upravleniya organizatsionnymi sistemami [Management theory of organizational systems]. Moscow, MPSI Publ., 2005, 584 p. (In Russian).
9. Kocynyak M. A., Kuleshov I. A., Kudryavcev M. A., Lauta O. S. *Kiberustojchivost informacionno-telekommunikacionnoj seti: monografiya* [Cyber stability of information and telecommunication network: monograph]. St. Petersburg, Boston-spektr Publ., 2015, 150 p. (In Russian).
10. Kazakov V. I. Osnovy teorii topogeodezicheskogo obespecheniya boevyh dejstvij vojsk. [Fundamentals of topographic and geodetic support of combat operations]. Moscow, VIA Publ., 1977. pp. 32–36. (In Russian).
11. Mahutov N. A., Reznikov D. O., Petrov P. V. Assesment of complex technical systems robustness. *Problemy bezopasnosti i chrezvychajnyh situacii,* 2009, no. 3, pp. 47–66. (In Russian).
12. Minaev V. A, Korolev I. D., Muhortov V. V. Markov models of drones information systems protection. *Tekhnologii tekhnosfernoj bezopasnosti,* 2016, iss. 6 (70). (In Russian). Available at: http://agps-2006.narod.ru/ttb/2016-6/17-06-16.ttb.pdf (accessed 15.10.2018).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Минаев Владимир Александрович, д.т.н., профессор, Московский государственный технический университет им. Н. Э. Баумана, 105005, Москва, 2-я Бауманская ул., д. 5, тел.: +7 (916) 294-92-90, e-mail: mlva@yandex.ru.
Королев Игорь Дмитриевич, д.т.н., профессор, Краснодарское высшее военное училище им. генерала армии С. М. Штеменко, 350063, Краснодар, ул. Красина, д. 4, тел.: +7 (918) 311-46-21, e-mail: pi_korolev@mail.ru.
Екатерина Валентиновна Зеленцова, к.т.н., доцент, Московский государственный технический университет им. Н. Э. Баумана, 105005, Москва, 2-я Бауманская ул., д. 5, тел.: +7 (903) 715-49-99, e-mail: katez@mail.ru.
Захарченко Роман Иванович, к.т.н., докторант, Краснодарское высшее военное училище им. генерала армии С. М. Штеменко, 350063, Краснодар, ул. Красина, д. 4, тел.: +7 (967) 659-71-25, e-mail: romanzakharchenko@yandex.ru.

AUTHORS

Vladimir A. Minaev, Dr.Sci. (Engineering), professor, Bauman Moscow State Technical University, 5, 2-ya Baumanskaya ulitsa, Moscow, 105005, Russia, tel.: +7 (916) 294-92-90, e-mail: mlva@yandex.ru.
Igor D. Korolev, Dr.Sci. (Engineering), professor, Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, 4, ulitsa Krasina, Krasnodar, 350063, Russia, tel.: +7 (918) 311-46-21, pi_korolev@mail.ru.
Ekaterina V. Zelentzova, Ph.D. (Engineering), associate professor, Bauman Moscow State Technical University, 5, 2-ya Baumanskaya ulitsa, Moscow, 105005, Russia, tel.: +7 (903) 715-49-99, e-mail: katez@mail.ru.
Roman I. Zakharchenko, Ph.D. (Engineering), doctoral student, Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, 4, ulitsa Krasina, Krasnodar, 350063, Russia, tel.: +7 (967) 659-71-25, e-mail: romanzakharchenko@yandex.ru.

Поступила 21.09.2018; принята к публикации 08.10.2018; опубликована онлайн 23.11.2018.
Submitted 21.09.2018; revised 08.10.2018; published online 23.11.2018.