DOI: 10.25586/RNU.V9187.18.11.P.129 УДК 004.056

**В.А. Минаев, А.В. Крупенин, И.Д. Королев,
К.М. Бондарь, Р.И. Захарченко**

ОЦЕНКА УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье рассматривается подход к оценке критической информационной инфраструктуры (КИИ), функционирующей в киберпространстве в условиях противоборства. Результатом оценки выступает значение интегрального критерия способности выполнения целевой функции КИИ в каждый момент времени. Новизной работы является перспективный метод оценки сложных технических систем, имеющих высокую степень критичности и неопределенности описания. Практическая значимость состоит в том, что новый метод оценки может быть использован для повышения эффективности управления КИИ, а также для обоснования новых форм и способов противоборства в киберпространстве. В статье рассматриваются вопросы кибернетической устойчивости, ее основные компоненты, свойства управления, определяющие киберустойчивость. Осуществлена классификация объектов критической информационной инфраструктуры. Дано формальное определение показателя киберустойчивости и приведены методика и алгоритм его расчета.

Ключевые слова: *кибернетическое пространство, информационное противоборство, компьютерные атаки, киберустойчивость, деструктивное информационное воздействие.*

**V.A. Minaev, A.V. Krupenin, I.D. Korolev,
K.M. Bondar, R.I. Zakharchenko**

ESTIMATION OF CRITICAL INFORMATION INFRASTRUCTURE SUSTAINABILITY FUNCTIONING

The article discusses the approach to the assessment of critical information infrastructure (CII), operating in cyberspace in conditions of information warfare. The result of assessment is the value of the integral criterion of ability to achieve goal function CII at each moment of time. The novelty of work is determined by the consideration of promising evaluation method of complex technical systems with a high degree of criticality and uncertainty representation. The practical significance consists in the fact that the new evaluation method can be used to improve the efficiency of management CII, and to justify new forms and methods of warfare in cyberspace. The article deals with the issues of cybernetic sustainability, its core components, and properties of management determining the cyber stability. Classification of CII objects is done. The formal definition of the cyber stability measure, the technique and the algorithm of its calculation are given.

Keywords: *cyberspace, information warfare, computer attacks, cyber stability, destructive informational influence.*

Введение

Высокая степень автоматизации управления, глобализация информационных систем (ИС), 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; 3]. При этом речь идет об искусственных воздействиях и искусственной среде его существования, порождающих, в свою очередь, новые де-факто сложившиеся, но юридически незакрепленные в Российской Федерации термины и их трактовку. Хотя уже появились работы по исследованию понятийного аппарата в данной области [4; 5].

Доступность через киберпространство критической информационной инфраструктуры (КИИ), под которой понимается совокупность автоматизированных систем управления и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач управления организационно-техническими системами, делает ее уязвимой от угроз, возникающих в киберпространстве (киберугроз), и ставит в зависимость от степени ее защищенности. Кроме того, защищенность КИИ напрямую зависит от владения соответствующими структурами новым видом оружия – кибероружием, отвечающим среде ее функционирования, от степени его эффективности, методов использования и средств защиты этого оружия. Именно все перечисленное создает необходимые предпосылки возникновения и осуществления эффективного противостояния в киберпространстве.

Кибернетическое оружие, вырабатывающее деструктивные информационные воздействия (ДИВ), не является оружием в классическом смысле, так как не осуществляет физическое поражение объекта атаки, а переводит его ИС и АСУ в критический режим функционирования.

Кибернетическое противостояние представляет собой процесс противодействия как минимум двух сторон, осуществляемого при совместном использовании общего ресурса (глобального информационного пространства), управление которым рассматривается как целенаправленное воздействие двух (и более) подсистем управления, стремящихся распространить эти управляющие воздействия друг на друга (рис. 1).

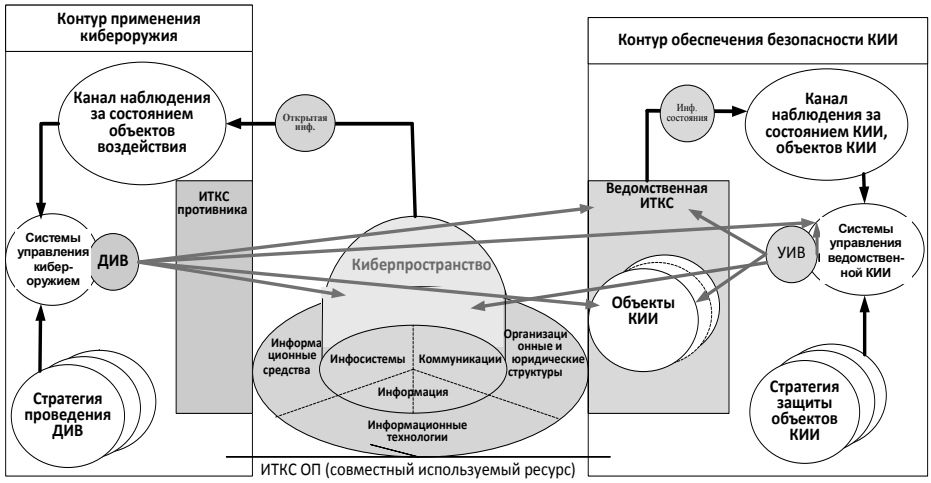

Рис. 1. Модель информационного противостояния в кибернетическом пространстве

Нарушение функционирования объектов КИИ в результате противостояния в киберпространстве может привести к различным эффектам – от временной потери управления объектом до физического разрушения объектов КИИ. Так, по оценке

экспертов [6], эффект целевого применения кибернетического оружия против ИС сравним с эффектом применения оружия массового поражения.

Таким образом, функционирование объектов КИИ в киберпространстве порождает новые уязвимости и угрозы и требует создания нового инструментария обеспечения безопасности КИИ, под которой понимается состояние ее защищенности, обеспечивающее устойчивое функционирование в условиях ДИВ любой интенсивности [4].

Проблема устойчивости критической информационной инфраструктуры

Как же оценить устойчивость функционирования такой сложной организационно-технической системы, как критическая информационная инфраструктура?

Анализ научной литературы, проведенный в работе [4], посвященной обеспечению безопасности КИИ, надежности и устойчивости функционирования АСУ объектов КИИ, показал, что в исследованиях практически не рассмотрены вопросы, связанные с разработкой моделей, методов и методик:

• оценки состояния объектов КИИ;

• формирования признакового пространства функционирования КИИ;

• формирования и ведения единой распределенной БД с оперативной аналитической обработкой данных;

• адаптивного управления КИИ, учитывающих текущее и прогнозируемое состояние объектов этой инфраструктуры в условиях ДИВ.

Кроме того, слабо разработан научно-методический аппарат построения автоматической системы сбора и приведения к единому виду информации, характеризующей состояние КИИ в условиях ДИВ.

Из сказанного следует, что существует необходимость в разработке подходов к созданию системы оценки устойчивости функционирования КИИ в условиях кибернетического противоборства. При этом надо отметить, что, несмотря на существенные упрощения, модель, представленная на рис. 1, позволяет сформулировать и описать важнейшие качества и свойства управления, определяющие киберустойчивость [4; 8; 9] (рис. 2).

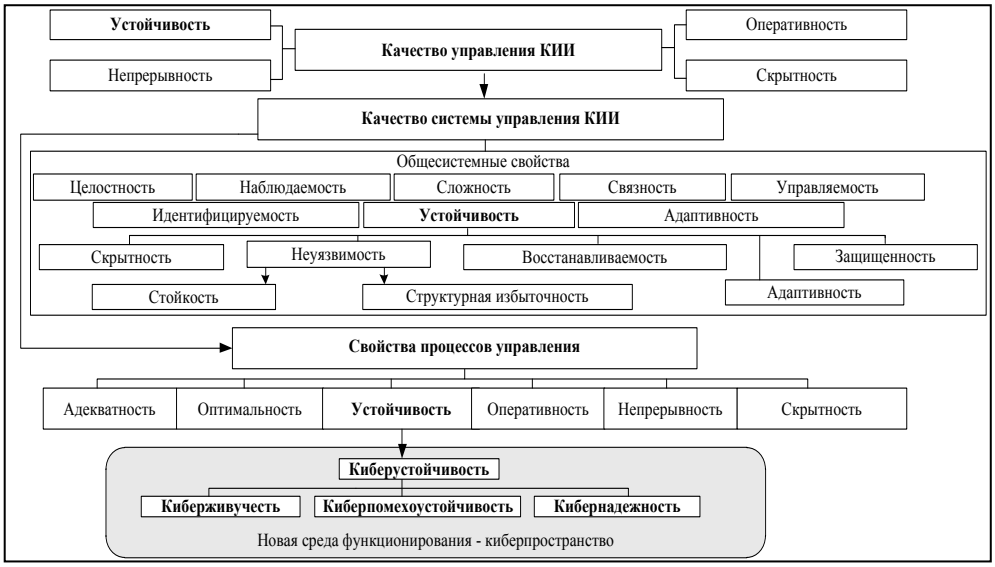

Рис. 2. Качества и свойства управления, определяющие киберустойчивость

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

Киберустойчивость

Если с устойчивостью в техносфере и инфосфере все более или менее определено, то с устойчивостью в киберпространстве (киберустойчивостью) возникает ряд вопросов, связанных с виртуальностью указанной среды. Причем процессы, происходящие в ней, оказывают прямые или косвенные воздействия, сказывающиеся на устойчивости функционирования КИИ в техносфере и инфосфере.

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

Классификация объектов критической информационной инфраструктуры

Существуют достаточно разнообразные объекты КИИ, и для дальнейшего их рассмотрения целесообразно произвести их классификацию по признакам (рис. 3), влияющим на обеспечение киберустойчивости функционирования.

Рис. 3. Слагаемые обеспечения киберустойчивости критической информационной инфраструктуры

1. По структурной организации – однозвенные и многозвенные.

Однозвенный объект КИИ – это объект, обладающий всеми необходимыми возможностями для выполнения единичной целевой функции (самостоятельный базовый элемент). Примером однозвенной структуры могут выступать отдельные комплексы средств автоматизации.

Многозвенный объект КИИ – объект, представляющий собой структурное последовательное объединение нескольких однозвенных объектов КИИ в единую систему в рамках выполнения единой целевой функции.

2. По функциональному единству – многозвенные однородные и многозвенные неоднородные.

Многозвенный однородный объект КИИ – объект, представляющий собой структурное последовательное объединение нескольких однозвенных объектов КИИ, выполняющих одинаковую целевую функцию, в единую систему в рамках выполнения единой целевой функции.

Многозвенный разнородный объект КИИ – объект, представляющий собой структурное последовательное объединение нескольких однозвенных объектов КИИ, выполняющих разные функции, например информационно-телекоммуникационную сеть, информационные системы и т.д.

Приведенная классификация помогает оценить киберустойчивость сложных организационных систем как совокупности взаимосвязанных (с учетом коэффициента связанности) однозвенных объектов КИИ (с учетом индивидуального вклада 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

Обобщенный показатель киберустойчивости однозвенного объекта ($К_{ОКИИуо}$) КИИ в данном случае имеет вид:

$$К_{ОКИИуо} = К_{ОКИИжив} К_{ОКИИпом} К_{ОКИИнад}, \quad (1)$$

где $К_{ОКИИжив}$ – киберживучесть КИИ, трактуемая как вероятность сохранения ее объектом работоспособности (выживания) в условиях выхода из строя технических средств обработки информации, т.е. по сути отражает вклад каждого элемента однозвенного объекта КИИ в выполнение им целевой функции;

$К_{ОКИИпом} = (1 – Р_{ПКА})(1 – Р_{ПЦКА})$ – киберпомехоустойчивость однозвенного объекта КИИ, понимаемая как вероятность выполнения целевой функции объекта КИИ с заданным качеством в условиях применения общих и целенаправленных деструктивных информационных воздействий; $Р_{ПКА}$ и $Р_{ПЦКА}$ – вероятности поражения технических средств обработки информации, входящих в объект КИИ, общими и целенаправленными деструктивными информационными воздействиями соответственно;

$К_{ОКИИнад}$ – кибернадежность однозвенного объекта КИИ, трактуемая как вероятность обеспечения выполнения целевой функции объекта КИИ на протяжении определенного временного интервала в условиях возникновения различных событий ($i = 1,\ldots, N$) – программных ошибок, технических сбоев и непреднамеренных ошибочных действий технического персонала и должностных лиц объекта КИИ, определяемая как:

$$К_{ОКИИнад} = \prod_{i=1}^{N} К_{ОКИИнад i} (1 – Р_i), \quad (2)$$

где $Р_i$ – вероятность i-го события ($i = 1, \ldots, N$).

К объектам КИИ уже на этапе проектирования закладываются довольно жесткие требования по технической надежности, и предусматривается ряд специальных мер по повышению оперативности устранения технических и программных отказов технических средств обработки информации (например, за счет кластеризации серверов, за счет резервирования отдельных обладающих низкой надежностью компонентов технических средств обработки (ТСОИ)). В соответствии с этим в задачах оценки киберустойчивости КИИ в условиях ДИВ вполне допустимо считать вероятность технических отказов ТСОИ при своевременном и качественном проведении технического обслуживания пренебрежительно малой. В данном случае кибернадежность однозвенного объекта КИИ будет определяться следующей формулой:

$$К_{ОКИИуо} = К_{ОКИИжив} К_{ОКИИпом}. \quad (3)$$

Если считать выходы из строя звеньев КИИ в условиях ДИВ независимыми событиями, то киберустойчивость многозвенного объекта ($К_{ОКИИум}$) КИИ может быть найдена из выражения:

$$К_{ОКИИум}(N) = \prod_{i=1}^{N} К_{ОКИИуо i}. \quad (4)$$

В противном случае киберустойчивость многозвенного объекта КИИ должна рассчитываться как совместная N-мерная вероятность сохранения работоспособности одновременно N звеньев, составляющих данный объект:

$$К_{ОКИИум}(N) = Р\{К_{ОКИИуо i} \geq К_{ОКИИуодоп}, \ldots, К_{ОКИИуо N} \geq К_{ОКИИуодоп}\}, \quad (5)$$

где для каждого i-го события ($i = 1, \ldots, N$) введены допустимые значения вероятностей.

Как следует из выражений (3) и (4), основой расчета киберустойчивости объектов КИИ является расчет показателей киберпомехоустойчивости и киберживучести отдельных звеньев объекта КИИ. Причем определяющим свойством с точки зрения возможности выполнения объектом КИИ целевой функции будет киберживучесть, а киберпомехоустойчивость выступает ее составной частью.

Способ оценки киберживучести объектов КИИ

В связи с тем, что свойства, характеризующие киберживучесть объекта КИИ при осуществлении ДИВ – Ω, начинают проявляться только после того, как она подверглась воздействию, то мера живучести должна определяться условной вероятностью сохранения работоспособности при условии, что система получила локальное повреждение [10].

Под показателем киберживучести однозвенного объекта $К_{ОКИИжив}$ будем понимать условную вероятность невыхода его конечного состояния за границы заданной области безопасных состояний S^I пространства S в случае ДИВ.

$$К_{ОКИИжив} = P\left[(\|S - s_0\| < S^I) / \Omega \right]. \quad (6)$$

Исходя из понятия структурной уязвимости системы [11–13], под которой будем понимать вероятность выхода конечного состояния системы из заданной безопасной области $S^I - V_S$, справедливо соотношение:

$$К_{ОКИИжив} = 1 - V_s, \quad (7)$$

а в конкретной точке на исследуемом временном интервале:

$$К_{ОКИИжив}(t) = 1 - V_s(t). \quad (8)$$

Критерием оценки киберживучести однозвенного объекта КИИ будем считать выражение:

$$К^{тек}_{ОКИИжив}(t) \geq К^{тр}_{ОКИИжив}(t), \quad (9)$$

где $К^{тек}_{ОКИИжив}(t)$ – текущий уровень живучести однозвенного объекта КИИ, а $К^{тр}_{ОКИИжив}(t)$ – требуемый уровень его живучести в условиях осуществления ДИВ.

Используя выражения (5, 7, 9), определим следующий критерий способности объекта КИИ выполнять целевую функцию $W_б$ в условиях ДИВ:

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

Для определения общего коэффициента живучести $К_{ОКИИNжив}(t)$ (5, 6, 8, 10) введем следующие уровни киберживучести:

$$К_{ОКИИNжив}(t) = \begin{cases} К^{тек}_{ОКИИжив}(t) - К^{тр}_{ОКИИжив}(t) > 0 - \text{оптимальный уровень,} \\ К^{тек}_{ОКИИжив}(t) - К^{тр}_{ОКИИжив}(t) = 0 - \text{допустимый уровень,} \\ К^{тек}_{ОКИИжив}(t) - К^{тр}_{ОКИИжив}(t) < 0 - \text{критический уровень,} \\ К^{тек}_{ОКИИжив}(t) = 0 - \text{закритический уровень (нулевой).} \end{cases} \quad (11)$$

Методика оценки киберустойчивости

В общем виде методика оценки киберустойчивости представляется следующими тремя этапами.

1. Этап оценки киберустойчивости каждого объекта КИИ отдельно.

1.1. Оценка однозвенного объекта КИИ, связанная с нижеперечисленными процедурами.

Оценка киберпомехоустойчивости – вероятности выхода из строя *i*-го ТСОИ в условиях ДИВ.

Оценка коэффициента связанности *i*-го ТСОИ и его вклада в целевую функцию объекта КИИ.

Оценка киберживучести – предела состояний однозвенного объекта КИИ.

1.2. Оценка многозвенного объекта КИИ.

Оценка киберпомехоустойчивости – вероятности выхода из строя *j*-го однозвенного объекта КИИ в условиях воздействия ДИВ, включающая следующие процедуры:

– оценка коэффициента связанности *j*-го однозвенного объекта КИИ и его вклада в целевую функцию многозвенного объекта КИИ;

– оценка киберживучести – предела состояний многозвенного объекта КИИ.

2. Этап оценки киберустойчивости взаимодействующих объектов КИИ.

Оценка киберпомехоустойчивости – вероятности выхода из строя *n*-го многозвенного объекта КИИ в условиях воздействия ДИВ.

Оценка коэффициента связанности *n*-го многозвенного объекта КИИ и его вклада в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести.

3. Этап оценки киберустойчивости КИИ через сумму устойчивости ее элементов с учетом коэффициента их связанности, включающий оценку киберживучести КИИ в динамике при выполнении ею своих функций.

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

Таким образом, в рамках разработки подхода к оценке устойчивости функционирования объектов КИИ предлагается расширить свойство устойчивости, являющегося интегральным, за счет применения нового вида оружия – кибероружия и, как следствие, появления новых уязвимостей и угроз для КИИ в целом и объектов КИИ. Предложенный способ за счет декомпозиции критической информационной структуры с выделением отдельных объектов КИИ с учетом их коэффициентов связанности и степени важности, выполняемых функций, позволяет оценить способность КИИ выполнять целевые функции. Полученный результат в соответствии с разработанной схемой отнесения класса состояния объекта к уровню качества (рис. 4) позволяет однозначно дать оценку устойчивости функционирования КИИ.

Выводы

1. Доступность критической информационной инфраструктуры влияет на ее защищенность, которая напрямую зависит от степени владения соответствующими структурами новым видом оружия – кибероружием, создающим необходимые предпосылки возникновения и осуществления эффективного противостояния в киберпространстве.

2. Функционирование объектов критической информационной инфраструктуры в киберпространстве порождает новые уязвимости и угрозы, требуя создания нового инструментария обеспечения безопасности КИИ, под которой понимается состояние ее защищенности, обеспечивающее устойчивое функционирование в условиях компьютерных атак любой интенсивности.

3. Объекты КИИ целесообразно классифицировать по признакам, влияющим на обеспечение киберустойчивости функционирования: по структурной организации – однозвенные и многозвенные; по функциональному единству – многозвенные однородные и многозвенные неоднородные.

4. Обобщенный показатель киберустойчивости включает показатели киберживучести, киберпомехоустойчивости и кибернадежности КИИ.

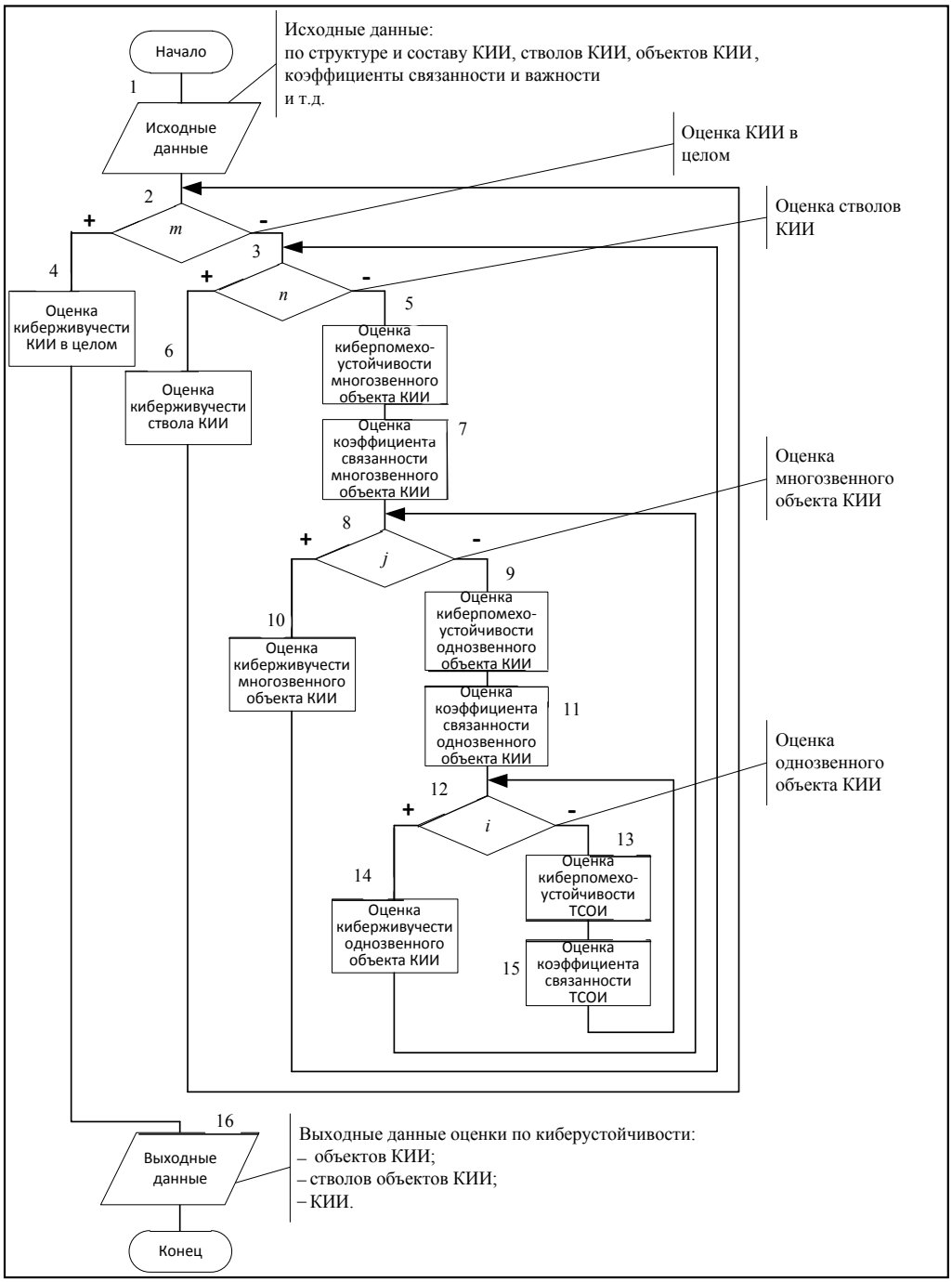

Рис 4. Блок-схема способа оценки устойчивости функционирования КИИ

5. Методика оценки киберустойчивости представляется тремя последовательными этапами:

• оценка киберустойчивости каждого объекта КИИ отдельно;

• оценка киберустойчивости взаимодействующих объектов КИИ;

• оценка киберустойчивости КИИ через сумму устойчивости ее элементов с учетом коэффициента их связанности, включая оценку киберживучести КИИ в динамике при выполнении ею своих функций.

Литература

1. *Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А.* Управление качеством информационных услуг / под общ. ред. Ю.И. Стародубцева. СПб.: Изд-во Политехнического университета, 2017. 454 с.

2. Глобальная безопасность в цифровую эпоху: стратагемы для России / под общ. ред. А.И. Смирнова. М.: ВНИИгеосистем, 2014. 394 с.

3. *Бедрицкий А.В.* Информационная война: концепции и их реализация в США / под ред. Е.М. Кожокина. М.: РИСИ, 2008. 187 с.

4. *Макаренко С.И., Чукляев И.И.* Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13–21.

5. *Фисун А.П., Касилов А.Г., Фисенко В.Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р.А., Джевага К.А., Кожухов С.А.* Развитие методологических основ информатики и информационной безопасности систем. Депонированная рукопись № 1165-В2004 07.07.2004. М.: ВИНИТИ, 2004. 253 с.

6. *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. Is. 3. P. 247–256.

7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».

8. *Боговик А.В., Игнатов В.В.* Теория управления в системах военного назначения: учебник. СПб.: ВАС, 2008. 460 с.

9. *Коцыняк М.А., Кулешов И.А., Кудрявцев М.А., Лаута О.С.* Киберустойчивость информационно-телекоммуникационной сети: монография. СПб.: Бостон-спектр, 2015. 150 с.

10. *Казаков В.И.* Основы теории топогеодезического обеспечения боевых действий войск. М.: ВИА, 1977.

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 // Интернет журнал «Технологии техносферной безопасности». 2016. Вып. 6 (70), Академия ГПС МЧС РФ [Электронный ресурс]. Режим доступа: http://ipb.mos.ru/ttb/2016-6.html (дата обращения: 28.11.17).

13. *Сафонов* Р.А. Методика оценки живучести сложных систем военного назначения [Электронный ресурс]. Режим доступа: http://www.xreferat.com/ 17/622-1-metodika-ocenki-zhivuchesti-slozhnyh-sistem-voennogo-naznacheniya.html (дата обращения: 28.11.17).

References

1. *Starodubtsev Yu.I., Begaev A.N., Davlyatova M.A.* Upravlenie kache-stvom informatsionnykh uslug / pod obshch. red. Yu.I. Starodubtseva. SPb.: Izd-vo Politekhnicheskogo universiteta, 2017. 454 s.

2. Global'naya bezopasnost' v tsifrovuyu epokhu: stratagemy dlya Rossii / pod obshch. red. A.I. Smirnova. M.: VNIIgeosistem, 2014. 394 s.

3. *Bedritskiy A.V.* Informatsionnaya voyna: kontseptsii i ikh realizatsiya v SSHA / pod red. E.M. Kozhokina. M.: RISI, 2008. 187 s.

4. *Makarenko S.I., Chuklyaev I.I.* Terminologicheskiy bazis v oblasti informatsionnogo protivoborstva // Voprosy kiberbezopasnosti. 2014. № 1 (2). S. 13–21.

5. *Fisun A.P., Kasilov A.G., Fisenko V.E., Minaev V.A., Afanas'ev V.V., Mityaev V.V., Fisun R.A., Dzhevaga* K.A., *Kozhukhov S.A.* Razvitie metodologicheskikh osnov informatiki i informatsionnoy bezopasnosti sistem. Deponirovannaya rukopis' № 165-V2004 07.07.2004. M.: VINITI, 2004. 253 s.

6. *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. Is. 3. P. 247–256.

7. Federal'nyy zakon ot 26.07.2017 № 187-FZ "O bezopasnosti kriti-cheskoy informatsionnoy infrastruktury RF".

8. *Bogovik A.V., Ignatov V.V.* Teoriya upravleniya v sistemakh voennogo naznacheniya: uchebnik. SPb.: VAS, 2008. 460 s.

9. *Kotsynyak M.A., Kuleshov I.A., Kudryavtsev M.A., Lauta O.S.* Kiberu-stoychivost' informatsionno-telekommunikatsionnoy seti: monografiya. SPb.: Boston-spektr, 2015. 150 s.

10. *Kazakov V.I.* Osnovy teorii topogeodezicheskogo obespecheniya boevykh deystviy voysk. M.: VIA, 1977.

11. *Makhutov N.A., Reznikov D.O., Petrov P.V.* Otsenka zhivuchesti slozh-nykh tekhnicheskikh sistem // Problemy bezopasnosti i chrezvychaynykh situatsiy. 2009. № 3. S. 47–66.

12. *Minaev V.A., Korolev I.D., Mukhortov V.V.* Markovskie modeli zashchity informatsionnykh sistem bespilotnykh robototekhnicheskikh ob"ektov // Internet zhurnal "Tekhnologii tekhnosfernoy bezopasnosti". 2016. Vyp. 6 (70), Akademiya GPS MCHS RF [Elektronnyy resurs]. Rezhim dostupa: http://ipb.mos.ru/ttb/2016-6.html (data obrashcheniya: 28.11.17).

13. *Safonov R.A.* Metodika otsenki zhivuchesti slozhnykh sistem voennogo naznacheniya [Elektronnyy resurs]. Rezhim dostupa: http://www.xreferat.com/ 17/622-1-metodika-ocenki-zhivuchesti-slozhnyh-sistem-voennogo-naznacheniya.html (data obrashcheniya: 28.11.17).