Раздел IV. Анализ данных и обработка информации

УДК 004:81, 004:052, 004:056.5 DOI 10.18522/2311-3103-2021-4-155-165

Е.А. Максимова, Н.П. Садовникова

ОЦЕНКА ИНФРАСТРУКТУРНОЙ УСТОЙЧИВОСТИ СУБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЯХ*

С принятием №187 ФЗ «О безопасности критической информационной инфраструктуры», реализация которого на практике не возможна без комплексной оценки информационной безопасности (ИБ) субъектов критической информационной инфраструктуры (СКИИ). Однако, существующие в настоящее время руководящие документы регуляторов не рассматривают СКИИ с точки зрения системного подхода, не учитывается инфраструктурная составляющая СКИИ при построении системы защиты информации. В это же время, оценка ИБ СКИИ без учета влияния на состояния и поведение системы возникающих в системе межобъектных и межсубъетных связей приводит к погрешности оценки, так как сама система при определенных условиях может генерировать деструктивизм инфраструктурного характера. Таким образом, погрешность в оценке ИБ СКИИ возникает за счет не учета показателя неспособности СКИИ реализовывать свой функционал в полном объеме под воздействием рисков инфраструктурного характера, т.е. инфраструктурного деструктивизма. С точки зрения теории устойчивости, данный показатель можно соотнести с категорией «инфраструктурная устойчивость СКИИ». Предлагаемая авторами исследования модель оценки инфраструктурной устойчивости (ИУ) СКИИ представлена 1) с использованием аппарата когнитивного моделирования, 2) с использованием аппарата теории надежности технических систем. В рамках когнитивного моделирования, значение концептов задается экспертно. В представленном исследовании для данной оценки предложено использовать аппарат логико-вероятностного моделирования, путем четкой структуризации системы – СКИИ. Таким образом, оценка инфраструктурной устойчивости СКИИ характеризуется возможностью оценивания вероятности безотказной работы объектов КИИ и предотвращения сбоев в функционировании сфер КИИ, что гарантирует стабильность и требуемый уровень ИБ. Проблема оценки ИУ в данном случае приобретает ключевой характер при комплексной оценке ИБ СКИИ.

Критическая информационная инфраструктура; деструктивные воздействия; инфраструктурная устойчивости; инфраструктурный деструктивизм; надежность; субъект; объект; модель; концепт; когнитивная модель; информационная безопасность.

E.A. Maksimova, N.P. Sadovnikova

DESTRUCTURIZATION OF CRITICAL INFORMATION INFRASTRUCTURE FOR ASSESSING THE INFRASTRUCTURAL STABILITY OF THE SUBJECT OF CRITICAL INFORMATION INFRASTRUCTURE UNDER DESTRUCTIVE INFLUENCES

With the adoption of Federal Law No. 187 "On the Security of Critical Information Infrastructure", the implementation of which in practice is not possible without a comprehensive assessment of information security (IS) of subjects of critical information infrastructure (SCII).

* Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ, проект № 3/2020).

However, the currently existing regulatory documents of regulators do not consider SCII from the point of view of a systematic approach, the infrastructural component of SCII is not taken into account when building an information protection system. At the same time, the assessment of IS SCII without taking into account the effect on the state and behavior of the system of inter-object and intersubject connections arising in the system leads to an error in the assessment, since the system itself, under certain conditions, can generate infrastructural destructivism. Thus, the error in assessing the ISSII arises due to the failure to take into account the indicator of the SCII's inability to implement its functionality in full under the influence of infrastructure risks, i.e. infrastructural destructivism. From the point of view of the theory of sustainability, this indicator can be correlated with the category of "infrastructure sustainability of SCII". The proposed by the authors of the study, the model for assessing the infrastructure sustainability (IS) of SCII is presented 1) using the apparatus of cognitive modeling, 2) using the apparatus of the theory of reliability of technical systems. Within the framework of cognitive modeling, the power of concepts is set by experts. In the presented study, for this assessment, it is proposed to use the apparatus of logical-probabilistic modeling, through a clear structuring of the system - SCII. Thus, the assessment of the infrastructure stability of the SCII is characterized by the possibility of assessing the probability of no-failure operation of the facilities of the CII and preventing failures in the functioning of the CII spheres, which guarantees stability and the required level of information security. In this case, the problem of assessing IS in this case acquires a key character in the comprehensive assessment of IS SCII.

Critical Information Infrastructure; destructive influences; infrastructure sustainability; infrastructural destructivism; reliability; subject; object; model; concept; cognitive model; Information Security..

Введение. В 2017 году принят №187 ФЗ «О безопасности критической информационной инфраструктуры» [1], реализация которого на практике не возможна без комплексной оценки информационной безопасности (ИБ) субъектов критической информационной инфраструктуры (СКИИ). Однако, существующие в настоящее время руководящие документы регуляторов не рассматривают СКИИ с точки зрения системного подхода, не учитывается инфраструктурная составляющая СКИИ при построении системы защиты информации. В это же время, оценка ИБ СКИИ без учета влияния на состояния и поведение системы возникающих в системе межобъектных и межсубъетных связей приводит к погрешности оценки, так как сама система при определенных условиях может генерировать деструктивизм инфраструктурного характера.

Когнитивная оценка инфраструктурного деструктивизма СКИИ. С целью повышения точности оценки ИБ СКИИ предлагается использовать методологию когнитивного моделирования [2–9]. В разработанной когнитивной модели «Оценка информационной безопасности субъекта КИИ» [10–12] кроме регулятивных составляющих, регламентированных в документе [13], предусматривается влияние на целевой концепт факторов, связанных с деструктивными воздействиями инфраструктурного характера.

К таким факторам, к примеру, отнесены ошибки инфраструктурного характера, не учет межобъектных связей в среде функционирования субъекта КИИ, наличие деструктивно-образующих межобъектных связей, факторы риска безопасности СКИИ, связанные с межсубъектными связями и др., являющиеся концептами третьего уровня обозначенной модели – составляющие оценки инфраструктурного деструктивизма (ИД) СКИИ (концепт второго уровня модели «Оценка ИБ СКИИ»). Формализация этих процессов представлена когнитивной моделью «Оценка инфраструктурного деструктивизма субъекта КИИ» (рис. 1). Составляющие данной модели - концепты: V1: «Оценка инфраструктурного деструктивизма субъекта КИИ», V1:1 «Ошибки, связанные с развитием СЗИ СКИИ на разных этапах жизненного цикла», V1:1 -1 «Ошибки, связанные с первичной разработкой информационной инфраструктуры организации (предприятия)», V1: 1-2 «Ошибки

в проектировании системы защиты СКИИ», V1:1-3 «Ошибки при реализации системы защиты субъекта КИИ», V1:1-4 «Ошибки при внедрении системы защиты субъекта КИИ», V1:1-5 «Отсутствие (не корректное построение) системы разграничения доступа в среде субъекта КИИ второго уровня», V1:2 «Инфраструктурные ошибки при развитии СКИИ», V1:2-1 «Ошибки при сопровождении субъекта КИИ», V1: 2-2 «Реализация атаки на объект КИИ», V1: 2-3 «Ошибки при анализе требований для субъекта КИИ», V1:2-4 «Ошибки, связанные с определением перечня объектов, подлежащих категорированию», V1:3 «Факторы рисков безопасности СКИИ, связанные с межобъектными связями», V1:3-1 «Ошибки инфраструктурного анализа», V1:3-2 «Не учет межобъектных связей в среде субъекта КИИ», V1:3-3 «Снижение уровня безопасности межобъектного взаимодействия», V1:3-4 «Инфраструктурное возмущение системы», V1:3-5 «Наличие деструктивнообразующих межобъектных связей», V1:3-5-1 «Наличие инфраструктурной связи типа «Облигативный симбиоз», V1:3-5-2 «Наличие инфраструктурной связи типа «Факультативный симбиоз», V1:3-5-3 «Наличие инфраструктурной связи типа «Комменсализм», V1:3-5-4 «Наличие инфраструктурной связи типа «Нейтрализм», V1:3-5-5 «Наличие инфраструктурной связи типа «Аменсализм», V1:3-5-6 «Наличие инфраструктурной связи типа «Аллелопатия», V1:3-5-7 «Наличие инфраструктурной связи типа «Конкуренция», V1:4 «Факторы рисков безопасности СКИИ, связанные с межсубъектными связями», V1:4-1 «Не учет межсубъектных отношений в среде функционирования КИИ», V1:4-2 «Снижение уровня безопасности хотя бы одного из взаимодействующих субъектов КИИ», V1:4-3 «Снижение уровня безопасности межсубъектного взаимодействия», V1:4-4 «Наличие прямых межсубъектных связей», V1:4-5 «Наличие косвенных межсубъектных связей».

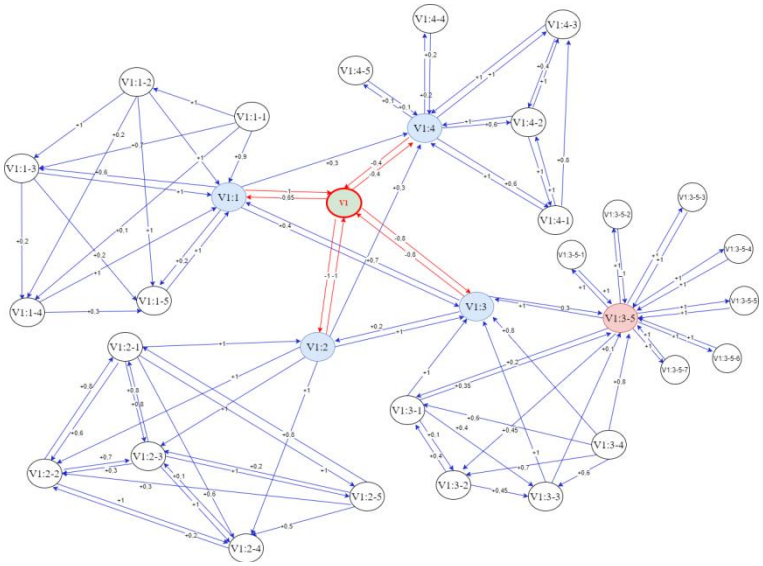

Рис. 1. Когнитивная модель «Оценка инфраструктурного деструктивизма субъекта КИИ»

Здесь, под инфраструктурным деструктивизмом СКИИ будем понимать показатель неспособности СКИИ реализовывать свой функционал в полном объеме под воздействием рисков инфраструктурного характера. С точки зрения теории устойчивости данный показатель можно соотнести с категорией «инфраструктурная устойчивость СКИИ».

Устойчивость СКИИ как системы. Теория устойчивости систем сегодня активно развивается и используется при решении широкого круга задач из разных сфер деятельности [14]. Согласно интерпретации толкового словаря Ушакова [15] «устойчивый – не поддающийся, не подверженный колебаниям и изменениям». Применительно к техническим системам «устойчивость» трактуется как возможность возврата системы в исходное состоянit после воздействия на нее.

М.Д. Гродзинский (1987) выделил три формы проявления устойчивости: инертность, восстанавливаемость, пластичность. Наличие рассматриваемых форм проявления устойчивости позволяет выделить два вида устойчивости: инертную (статическую) и упругую [14]. Вид устойчивости отражает не только временной аспект, он непосредственно взаимосвязан и с характеристикой системы [16]. Таким образом, инфраструктурную устойчивость определим, как способность инфраструктуры при возмущении системы оставаться на заданном качественном уровне на фоне высокого уровня инфраструктурного деструктивизма. В качестве «возмущений системы» на уровне СКИИ, в том числе будем рассматривать изменение инфраструктуры за счет добавления (удаления) объекта (объектов) КИИ.

Инфраструктурная устойчивость СКИИ проявляется в инертной форме и в контексте когнитивного моделирования ИБ СКИИ может рассматриваться как мера силы концепта «Оценка функциональности СКИИ» [10, 11].

Оценка данного показателя в настоящее время рассматривается как самостоятельная величина. Так, например, в работе [17] представлена схема обеспечения устойчивости функционирования КИИ в условиях угроз комплексных информационно-технических воздействий и информационно-психологических воздействий, приводящих к компьютерным инцидентам в КИИ, Данная схема основана на том, что элементы КИИ являются «человеко-машинными» взаимосвязанными системами, в которых информационное воздействие на человека и/или компьютеризированные, роботизированные средства приводит к снижению эффективности КИИ в целом.

Вопросы зависимости устойчивости инфраструктуры от топологии рассмотрены в [18, 19]. Обосновано это тем, что мониторинг и оценка состояния, а также, в конечном счете, задачи более высокого порядка требуют своевременных и точных измерений. Знание текущей топологии системы имеет решающее значение для интерпретации любых таких измерений, а также требуется для оценки состояния для получения правильных результатов. Поскольку как ошибки, так и преднамеренные действия могут изменить топологию, важным шагом в любой оценке состояния является получение наиболее адекватной структуры для заданного набора измерений. Это, однако, обычно выполняется до оценки состояния. Данный подход может позволить, к примеру, сформулировать задачу оптимизации для минимизации затрат для предотвращения злоумышленных последствий и определить последствия индуцированных сбоев топологии, приводящих к атакам типа "отказ в обслуживании" вплоть до потери наблюдаемости и возможности восстановления исследования.

Определение меры инфраструктурной устойчивости. Достаточно близким к понятию «устойчивость» является понятие «надежность», но она характеризуется обычно как мера вероятности устойчивой работы, вероятности безотказной работы [14].

В контексте данного исследования, так как решается задача, связанная с определением меры инфраструктурной устойчивости, то на инфраструктурном уровне данная задача может быть решена путем оценки надежности рассматриваемой системы.

В рамках когнитивного моделирования, традиционно, значения концептов задается экспертно. В это же время, на наш взгляд, возможна ее оценка с использованием аппарата логико-вероятностного моделирования, путем четкой структуризации системы – СКИИ.

Исследование инфраструктурной устойчивости СКИИ. Структуризацию СКИИ как системы можно реализовать с помощью деструктуризации инфраструктуры соответствующего субъекта и определения топологических особенностей полученных подсистем.

При декомпозиции структуры СКИИ, согласно [20] можно выделить:

1. Односвязную декомпозицию структуры.

2. Многосвязную декомпозицию.

3. Декомпозицию, связанную с разложением по полной группе событий относительно выделенных элементов, блоков и др.

4. Логическую декомпозицию.

Применительно к КИИ возможны следующие формы декомпозиции системы:

1) на уровне КИИ – для межсубъектного взаимодействия – 1,2,4 формы декомпозиции;

2) на уровне СКИИ – только вариант 3.

Таким образом, на уровне субъекта КИИ рассматриваем три варианта декомпозиции: регулятивная декомпозиция (однослойная) – пообъектная декомпозиция СКИИ, двухслойная декомпозиция СКИИ – декомпозиция на уровне одного субъекта КИИ выполненная путем объединения взаимодействующих объектов в подсистемы. При данном варианте декомпозиции внешнее воздействие на элементы СКИИ не учитываются, двухслойная декомпозиция СКИИ – декомпозиция на уровне взаимодействующих субъектов КИИ с одновременным выполнением двухслойной декомпозиции взаимодействующих субъектов.

Для исследования инфраструктурной устойчивости СКИИ при деструктивных воздействиях кроме того необходимо сформулировать принципы выполнения декомпозиции СКИИ на подсистемы взаимодействующих объектов:

1) Принцип связности: составляющие (объекты КИИ) данной подсистемы находятся в отношении «быть связанным».

2) Принцип однозначности: в данном СКИИ нет ни одного объекта КИИ, который бы принадлежал более чем одной подсистеме взаимодействующих объектов.

3) Принцип целостности: Совокупность всех элементов подсистем взаимодействующих объектов составляет СКИИ.

4) Принцип статичности: в статичном режиме состав и структура СКИИ остается неизменной.

5) Принцип возмущения системы: возмущение системы возникает в результаты изменения состава инфраструктуры субъекта.

6) Принцип инфраструктурного деструктивизма: деструктивные воздействия приводят к инфраструктурным изменениям, что проявляется на уровне уязвимой подсистемы взаимодействующих объектов и безопасности СКИИ как системы.

7) Принцип инфраструктурного единообразия: в стационарном режиме состав и структура СКИИ остаются неизменными.

8) Принцип смягчения инфраструктурного деструктивизма: инфраструктурный деструктивизм, вызванный возмущением системы, возможно «смягчить» путем инфраструктурной декомпозиции. Инфраструктурная декомпозиция в данном случае выполняется путем оптимизации «возмущенной» инфраструктуры по критериям, специфичным для данного типа «возмущения».

В теории надежности технических систем перечисленные схемы декомпозиции являются базовыми. С помощью них и при использовании аппарата структурно-логического анализа можно выйти на оценку основных характеристик надежности исследуемого объекта, где не маловажную роль играет определение его структуры.

С этой точки зрения необходимо в структуре СКИИ выделить следующие группы элементов:

1) отказ которых практически не влияет на работоспособность системы;

2) работоспособность которых практически не изменяется и вероятность их безотказной работы близка к единице;

3) ремонт или регулировка которых возможны в процессе работы;

4) отказ которых приводит к отказу системы.

При анализе инфраструктурной устойчивости системы (ИУС) имеет смысл включать в рассмотрение элементы только последней группы. При расчете вероятности безотказной работы и других характеристик инфраструктурной устойчивости целесообразно воспользоваться структурно-логическими схемами надежности, в которых учитываются взаимосвязь элементов друг с другом и их влияние на работоспособность системы.

Таким образом, оценка ИУ СКИИ характеризуется возможностью оценивания вероятности безотказной работы объектов КИИ и предотвращения сбоев в функционировании сфер КИИ, что гарантирует стабильность и требуемый уровень ИБ. Проблема оценки ИУ в данном случае приобретает ключевой характер при комплексной оценке ИБ СКИИ.

Модель оценки инфраструктурной устойчивости СКИИ при деструктивных воздействиях. ИУ СКИИ зависит от следующих факторов:

- на уровне состава элементов СКИИ и их обслуживания,
- на уровне инфраструктуры субъекта.

Отказы объектов КИИ происходят вследствие воздействия различных факторов, к которым относятся физические, физико-химические и химические, биологические и эксплуатационные факторы, а также реализация угроз ИБ [21].

Предлагаемая модель оценки инфраструктурной устойчивости субъекта критической информационной инфраструктуры на уровне состава его элементов и их обслуживания представлена следующей функцией:

$$F = F\left(P_{thr}, P_{rel_i}\right),$$

где P_{reli} – вектор вероятностей безотказной работы объектов КИИ;

P_{thr} – вектор вероятностей наличия деструктивных воздействий.

Элементы P_{thr} могут принимать следующие значения:

$$P_{thr} = P_{Destr_i}, \quad P_{thr} = P_{exp},$$

где P_{Destri}– вероятность деструктивных воздействий на разных этапах жизненного цикла КИИ; P_{exp}– экспертная оценка вероятности реализации деструктивных воздействий.

В модели оценки ИУ СКИИ на уровне состава его элементов и их обслуживания P_{Destri} прогнозируется методом экстраполяции наименьших квадратов на основе существующей статистики на предприятиях и в организациях, функционирующих в сферах КИИ. В случае необходимости, предусматривается возможность ввода значения P_{exp}, отличного от прогнозируемого значения P_{Destri} на основе существующей статистики.

Возникновение деструктивных воздействий, на разных этапах ЖЦ СЗИ субъекта КИИ порождает уязвимости в системе защиты КИИ, которые злоумышленники могут эксплуатировать для реализации угроз на СКИИ.

Для оценки P_{exp} экспертом возможно использование значения частотной вероятности реализации угроз:

$$P_{exp} = \lim_{N \to \infty} \frac{n}{N},$$

где N – общее количество случившихся инцидентов за год; n – количество конкретных инцидентов за год.

Вероятность безотказной работы объектов КИИ P_{reli} зависит от вероятностей безотказной работы подобъектов КИИ и их взаимосвязей:

$$P_{\Re l_i} = P(InvU_1, InvU_2, InvU_3, InvU_7, InvU_9),$$

где $InvU_1$ – множество АРМ; $InvU_2$ – множество серверов; $InvU_3$ – множество АСО; $InvU_7$ – множество каналов связи; $InvU_9$ – множество подобъектов КИИ, специфичных для каждого отдельно взятого объекта КИИ.

В ходе исследования рассмотрены все показатели надежности восстанавливаемых и невосстанавливаемых подобъектов КИИ. Проведенный анализ показал, что для оценки надежности субъекта КИИ достаточным является показатель «вероятность безотказной работы».

Для реализации оценки надежности объектов КИИ P_{reli} рассмотрено три случая, где p_i– вероятность безотказной работы подобъектов КИИ:

1. Схема с последовательным соединением n зависимых подобъектов КИИ:

$$P_{\Re l_i} = \prod_{i=1}^{n} p_i\,(t).$$

2. Схема с параллельным соединением n зависимых подобъектов КИИ:

$$P_{\Re l_i} = 1 - \prod_{i=i}^{n} \left(1 - p_i \middle| (t)\right).$$

3. Последовательно – параллельная схема. Для оценки надежности объектов КИИ применяется поэтапное упрощение схемы и применение формул для оценки надежности схем с последовательным и параллельным соединением.

Оценка ИУ СКИИ P_{subj} рассчитывается аналогично схемам оценки надежности объектов КИИ: с применением расчетов для параллельного и последовательного соединения объектов КИИ. После оценки надежности объектов КИИ, для оценки ИУ КИИ осуществляется формирование структурной схемы взаимосвязи объектов КИИ и, исходя из вероятностей безотказной работы объектов КИИ и вероятности реализации угроз, рассчитывается оценка ИУ СКИИ.

$$P_{subj} = P_{\Re l_i} * (1 - P_{thr}).$$

В случае, если оценка ИУ СКИИ на уровне состава его элементов и их обслуживания недостаточная (P_{subj}<=0,5), то необходимо для ее повышения применить дополнительные меры, например, методы резервирования.

Для повышения оценки ИУ СКИИ применяются следующие методы и расчеты для резервирования подобъектов КИИ, где p_i– вероятность безотказной работы подобъектов КИИ:

1. При применении нагруженного резервирования (для системы с последовательным соединением *n* подобъектов при общем резервировании с кратностью *k),* надежность субъекта КИИ рассчитывается следующим образом:

$$P_{subj} = 1 - (1 - P)^{k+1} = 1 - (1 - \prod_{i=1}^{n} P_i(t))^{k+1}.$$

2. При применении нагруженного резервирования (для системы с последовательным соединением n объектов при раздельном резервировании с кратностью *k*), надежность субъекта КИИ рассчитывается следующим образом:

$$P_{subj} = \prod_{i=1}^{n}(1 - (1 - P_i(t))^{k+1}).$$

3. При применении ненагруженного резервирования (системы с ненагруженным резервированием кратности k (всего подобъектов k + 1)), надежность субъекта КИИ рассчитывается следующим образом:

$$P_{subj} = 1 - \frac{1}{(K+1)!}\prod_{i=1}^{k+1}\left(1 - P_i\right|(t)).$$

По результатам оценки ИУ СКИИ до резервирования и после резервирования осуществляется расчет коэффициента выигрыша надежности:

$$G_p = \frac{P_{before}}{P_{after}},$$

где P_{before} – оценка ИУ СКИИ до резервирования; P_{after}– оценка ИУ СКИИ после резервирования.

Для оценки уровня ИУ СКИИ на уровне состава его элементов и их обслуживания в качестве порогового значения выбрано значения 0,5. В случае значения данной оценки ниже 0,5, предлагаются рекомендации по ее повышению, которые включают методы нагруженного и ненагруженного резервирования.

Заключение. Погрешность в оценке ИБ СКИИ возникает за счет не учета показателя неспособности СКИИ реализовывать свой функционал в полном объеме под воздействием рисков инфраструктурного характера, т.е. инфраструктурного деструктивизма. С точки зрения теории устойчивости, данный показатель можно соотнести с категорией «инфраструктурная устойчивость СКИИ».

Предлагаемая модель оценки инфраструктурной устойчивости субъекта критической информационной инфраструктуры на уровне состава его элементов и их обслуживания представлена функцией, зависящей от значений вероятностей безотказной работы объектов КИИ и вероятностей наличия деструктивных воздействий в среде СКИИ.

Для повышения объективности при формировании когнитивной модели предлагается оценивать концепты с использованием аппарата логико-вероятностного моделирования, путем четкой структуризации системы – СКИИ.

Полученная оценка ИУ СКИИ позволяет оценивать вероятность безотказной работы объектов КИИ и предотвращать сбои в работе КИИ, что гарантирует стабильность и требуемый уровень ИБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017г. N 187-ФЗ (с изм. и доп.). – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.
2. *Робертс Ф.С.* Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам: пер. с англ. – М.: Наука, 1986. – 496 с.

3. *Kosko V.* Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. – 1986. – Vol. 24. – P. 65-75.
4. *Ажмухамедов И.М.* Информационная безопасность. Системный анализ и нечеткое когнитивное моделирование. – М.: Изд-во LAP, 2012. – 385 с.
5. *Ажмухамедов И.М.* Анализ и управление комплексной безопасностью на основе когнитивного моделирования // Управление большими системами. – 2010. – Вып. 29. – С. 5-15.
6. *Ажмухамедов И.М.* Динамическая нечѐткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. – 2010. – № 2. – С. 8-72.
7. *Садовникова Н.П., Жидкова Н.П.* Выбор стратегий территориального развития на основе когнитивного анализа и сценарного моделирования // Интернет-вестник ВолгГАСУ : серия Строительная информатика. – 2012. – № 7 (21). – URL: http://vestnik.vgasu.ru/attachments/SadovnikovaZhidkova-2012_7(21).pdf.
8. *Садовникова Н. П., Киктеев А.С.* Применение агентного моделирования для построения сценариев стратегического развития // Известия ВолгГТУ. Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах». – 2012. – № 4 (91). – С. 144-147.
9. *Дроботов А.С., Садовникова Н.П.* Применение метода имитационного моделирования для анализа рисков инновационного проекта // Системные проблемы надѐжности, качества, инф.-телекоммуникац. и электрон. технологий в управл. инновационными проектами: (Инноватика-2008): Матер. междунар. конф. и рос. науч. школы. Науч. центр «АСОНИКА» [и др.]. – М., 2008. – Ч. 2. – С. 20-22.
10. *Максимова Е.А.* Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Тр. учебных заведений связи. – 2020. – Т. 6, № 4. – С. 91-103. – DOI:10.31854/1813-324X-2020-6-4-91-103.
11. *Максимова Е.А.* Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях: монография: Федер. гос. авт. образоват. учреждение высш. образования «Волгогр. гос. ун-т»». – Волгоград: Изд-во ВолГУ, 2020. – 95 с.
12. *Maksimova E.A.* “Smart decisions” in development of a model for protecting information of a subject of critical information infrastructure // Lecture Notes in Networks and Systems. – 2021. – Vol. 155. – P. 1213-1221.
13. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства РФ от 8 февраля 2018 г. № 127 (не вступил в силу). – URL: https://www.garant.ru/products/ipo/prime/doc/71776120/.
14. *Косолапов О.В., Игнатьева М.Н.* Устойчивость как одна из основных характеристик системы // Известия Уральского государственного горного университета. – 2013. – № 4. – С. 77-81. – URL: https://e.lanbook.com/journal/issue/290438. – Загл. с экрана.
15. «Устойчивый -…». – URL: https:// dic.academic.ru/dic.nsf/ushakov/1071254.
16. *Казаков Л.К.* Ландшафтоведение. – М.: Изд. центр «Академия», 2011. – 336 с.
17. *Климов С.М., Поликарпов С.В., Рыжов Б.С., Тихонов Р.И., Шпырня И.В.* Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кибербезопасности. – 2019. – № 6 (34). – С. 37-48.
18. *Гаджиев Б.Р., Гибина Е.Ю., Прогулова Т.Б., Щетинина Д.П.* Топология и устойчивость локально-мировых сетей // Программные продукты и системы. – 2009. – № 4. – С. 51-54. – URL: https:// topologiya-i-ustoychivost-lokalno-mirovyh-setey.pdf.
19. *Балашова Т.И.* Обеспечение отказоустойчивости сети повышением надежности её топологии // Современные проблемы науки и образования. – 2014. – № 6. – URL: http://science-education.ru/ru/article/view?id=16846.
20. *Викторова В.С., Степанянц А.С.* Многоуровневое моделирование надежности систем // Датчики и системы. – 2014. – № 6 (181). – С. 33-37.
21. *Громов Ю.Ю., Иванова О.Г., Мосягина Н.Г., Набатов К.А.* Надежность информационных систем. – Тамбов: Изд-во ГОУ ВПО ТГТУ, 2010. – 5 с.

REFERENCES

1. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Federal'nyy zakon ot 26 iyulya 2017g. N 187-FZ (s izm. i dop.) [On the security of the critical Information Infrastructure of the Russian Federation: Federal Law No. 187-FZ of July 26, 2017 (ed. and add.)]. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/.
2. *Robertc F.S.* Diskretnye matematicheskie modeli s prilozheniyami k sotsial'nym, biologicheskim i ekologicheskim zadacham [Discrete mathematical models with applications to social, biological and environmental problems]: transl. from engl. Moscow: Nauka, 1986, 496 p.
3. *Kosko V.* Fuzzy Cognitive Maps, *International Journal of Man-Machine Studies*, 1986, Vol. 24, pp. 65-75.
4. *Azhmuhamedov I.M.* Informacionnaya bezopasnost'. Sistemnyj analiz i nechetkoe kognitivnoe modelirovanie [Information security. System analysis and fuzzy cognitive modeling.]. Moscow: Izd-vo LAP, 2012, 385 p.
5. *Azhmuhamedov I.M.* Analiz i upravlenie kompleksnoj bezopasnost'yu na osnove kognitivnogo modelirovaniya [Analysis and management of complex security based on cognitive modeling], *Upravlenie bol'shimi sistemami* [Managing large systems], 2010, Issue 29, pp. 5-15.
6. *Azhmukhamedov I.M.* Dinamicheskaya nechètkaya kognitivnaya model' vliyaniya ugroz na informatsionnuyu bezopasnost' sistemy [Dynamic fuzzy cognitive model of the impact of threats on the information security of the system], *Bezopasnost' informatsionnykh tekhnologiy* [Information technology security], 2010, No. 2, pp. 8-72.
7. *Sadovnikova N.P., Zhidkova N.P.* Vybor strategiy territorial'nogo razvitiya na osnove kognitivnogo analiza i stsenarnogo modelirovaniya [Selection of territorial development strategies based on cognitive analysis and scenario modeling], *Internet-vestnik VolgGASU : seriya Stroitel'naya informatika* [VolgGASU Internet Bulletin : Construction Informatics series], 2012, No. 7 (21). Available at: http://vestnik.vgasu.ru/attachments/SadovnikovaZhidkova-2012_7(21).pdf.
8. *Sadovnikova N.P., Kikteev A.S.* Primenenie agentnogo modelirovaniya dlya postroeniya stsenariev strategicheskogo razvitiya [Application of agent-based modeling to build strategic development scenarios], *Izvestiya VolgGTU. Seriya «Aktual'nye problemy upravleniya, vychislitel'noy tekhniki i informatiki v tekhnicheskikh sistemakh»* [Izvestiya VolgSTU. The series "Actual problems of management, computer engineering and computer science in technical systems"], 2012, No. 4 (91), pp. 144-147.
9. *Drobotov A.S., Sadovnikova N.P.* Primenenie metoda imitatsionnogo modelirovaniya dlya analiza riskov innovatsionnogo proekta [Application of the simulation modeling method for risk analysis of an innovative projec], *Sistemnye problemy nadèzhnosti, kachestva, inf.-telekommunikats. i elektron. tekhnologiy v upravl. innovatsionnymi proektami: (Innovatika-2008): Mater. mezhdunar. konf. i ros. nauch. shkoly. Nauch. tsentr «ASONIKA» [i dr.]* [Systemic problems of reliability, quality, information and telecommunication and electronic technologies in the management of innovative projects: (Innovatika-2008): Proceedings of the international conference and the Russian scientific school. Scientific Center "ASONIKA" [et al.]. Moscow, 2008, Part 2, pp. 20-22.
10. *Maksimova E.A.* Kognitivnoe modelirovanie destruktivnykh zloumyshlennykh vozdeystviy na ob"ektakh kriticheskoy informatsionnoy infrastruktury [Cognitive modeling of destructive malicious influences on objects of critical information infrastructure], *Tr. uchebnykh zavedeniy svyazi* [The works of the schools of communication], 2020, Vol. 6, No. 4, pp. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103.
11. *Maksimova E.A.* Otsenka informatsionnoy bezopasnosti sub"ekta kriticheskoy informatsionnoy infrastruktury pri destruktivnykh vozdeystviyakh: monografiya [Assessment of information security of a subject of critical information infrastructure under destructive influences: monograph]: Feder. gos. avt. obrazovat. uchrezhdenie vyssh. obrazovaniya «Volgogr. gos. un-t»». Volgograd: Izd-vo VolGU, 2020, 95 p.
12. *Maksimova E.A.* “Smart decisions” in development of a model for protecting information of a subject of critical information infrastructure, *Lecture Notes in Networks and Systems*, 2021, Vol. 155, pp. 1213-1221.
13. Ob utverzhdenii Pravil kategorirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe Perechnya pokazateley kriteriev znachimosti ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy:

Postanovlenie Pravitel'stva RF ot 8 fevralya 2018 g. № 127 (ne vstupil v silu) [On approval of the Rules for Categorizing Objects of Critical Information Infrastructure of the Russian Federation, as well as the List of Indicators of Criteria for the Significance of Objects of Critical Information Infrastructure of the Russian Federation and their Values: Decree of the Government of the Russian Federation of February 8, 2018 No. 127 (not entered into force)]. Available at: https://www.garant.ru/products/ipo/prime/doc/71776120/.

14. *Kosolapov O.V., Ignat'eva M.N.* Ustoychivost' kak odna iz osnovnykh kharakteristik sistemy [Stability as one of the main characteristics of the system], *Izvestiya Ural'skogo gosudarstvennogo gornogo universiteta* [Izvestiya Ural State Mining University], 2013, No. 4, pp. 77-81. Available at: https://e.lanbook.com/journal/issue/290438. Zagl. s ekrana.
15. «Ustoychivyy -…» ["Steady -..."]. Available at: https:// dic.academic.ru/dic.nsf/ushakov/ 1071254.
16. *Kazakov L.K.* Landshaftovedenie [Landscape studies]. Moscow: Izd. tsentr «Akademiya», 2011, 336 p.
17. *Klimov S.M., Polikarpov S.V., Ryzhov B.S., Tikhonov R.I., Shpyrnya I.V.* Metodika obespecheniya ustoychivosti funktsionirovaniya kriticheskoy informatsionnoy infrastruktury v usloviyakh informatsionnykh vozdeystviy [Methodology for ensuring the stability of the functioning of critical information infrastructure in the conditions of information impacts], *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2019, No. 6 (34), pp. 37-48.
18. *Gadzhiev B.R., Gibina E.YU., Progulova T.B., Shchetinina D.P.* Topologiya i ustoychivost' lokal'no-mirovykh setey [Topology and stability of local-world networks], *Programmnye produkty i sistemy* [Software products and systems], 2009, No. 4, pp. 51-54. Available at: https:// topologiya-i-ustoychivost-lokalno-mirovyh-setey.pdf.
19. *Balashova T.I.* obespechenie otkazoustoychivosti seti povysheniem nadezhnosti ee topologii [Ensuring network fault tolerance by increasing the reliability of its topology], *Sovremennye problemy nauki i obrazovaniya* [Modern problems of science and education], 2014, No. 6. Available at: http://science-education.ru/ru/article/view?id=16846.
20. *Viktorova V.S., Stepanyants A.S.* Mnogourovnevoe modelirovanie nadezhnosti sistem [Multilevel modeling of system reliability], *Datchiki i sistemy* [Sensors and systems], 2014, No. 6 (181), pp. 33-37.
21. *Gromov Yu.yu., Ivanova O.G., Mosyagina N.G., Nabatov K.A.* Nadezhnost' informatsionnykh system [Reliability of information systems]. Tambov: Izd-vo GOU VPO TGTU, 2010, 5 p.

Статью рекомендовал к опубликованию д.т.н., профессор И.М. Ажмухамедов.

Максимова Елена Александровна – Российский технологический университет МИРЭА (РТУ МИРЭА); e-mail: maksimova@mirea.ru; г. Москва, Россия; тел.: 89616982279; к.т.н.; доцент; доцент кафедры «Прикладные информационные технологии» института комплексной безопасности и специального приборостроения.

Садовникова Наталья Петровна – Волгоградский государственный технический университет, e-mail: npsn1@yandex.ru; г. Волгоград, Россия; тел.: 8917337652, д.т.н.; профессор; профессор кафедры "Системы автоматизированного проектирования и поискового конструирования".

Maksimova Elena Aleksandrovna – Russian Technological University MIREA (RTU MIREA), e-mail: maksimova@mirea.ru; Moscow, Russia; phone: +79616982279; the department "Applied Information Technologies" of the Institute of Integrated Security and Special Instrumentation; cand. of eng. sc.; associate professor.

Sadovnikova Natalia Petrovna – Volgograd State Technical University; e-mail: npsn1@yandex.ru; Volgograd, Russia; phone: +7917337652; the department of "Computer-aided Design and Search Design Systems"; dr. of eng. sc.; professor.