УДК 004.056 Вестник УрФО № 1(43) / 2022, с. 50–63

Максимова Е. А., Буйневич М. В.

DOI: 10.14529/secur220107

МЕТОД ОЦЕНКИ ИНФРАСТРУКТУРНОЙ УСТОЙЧИВОСТИ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье отмечается, что существующие в настоящее время подходы к обеспечению безопасности критической информационной инфраструктуры (КИИ) не рассматривают субъекты КИИ с точки зрения системного подхода и (или) не учитывают инфраструктурную составляющую КИИ при построении системы защиты информации. В это же время, сама система при определенных условиях может генерировать деструктивизм инфраструктурного характера. Предлагаемая авторами исследования модель оценки инфраструктурной устойчивости (ИУ) КИИ представлена на инфраструктурно-контекстном (оценка инфраструктурной надежности) и структурном (оценка инфраструктурной целостности) уровнях и является ключевым компонентом в комплексной оценке информационной безопасности КИИ. Представлено решение проблемы учета факторов, связанных с инфраструктурной устойчивостью КИИ в процессе анализа ИБ и обеспечения возможности прогнозирования деструктивных воздействий при различных изменениях информационной инфраструктуры.

Ключевые слова: *критическая информационная инфраструктура, деструктивное воздействие, инфраструктурная устойчивости, инфраструктурный деструктивизм, надежность, целостность, субъект, объект, когнитивная модель, информационная безопасность.*

Maksimova E. A., Buynivich M. V.

THE METHOD OF ASSESSING THE INFRASTRUCTURAL STABILITY OF THE SUBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

The article notes that currently existing approaches to ensuring the security of critical information infrastructure (CII) do not consider CII subjects from the point of view of a systematic approach and (or) do not take into account the infrastructure component of CII when building an information security system. At the same time, the system itself, under certain conditions, can generate infrastructural destructiveness. The model for assessing the infrastructure sustainability (IS) of CII proposed by the authors of the study is presented at the infrastructure-contextual (assessment of infrastructure reliability) and structural (assessment of infrastructure integrity) levels and is a key component in a comprehensive assessment of information security of CII. A solution to the problem of taking into account factors related to the infrastructural stability of CII in the process of IS analysis and providing the possibility of predicting destructive impacts with various changes in the information infrastructure is presented.

Keywords: *critical information infrastructure, de-structive impact, infrastructural sustainability, infrastructural destructivism, reliability, integrity, subject, an object, cognitive model, Information Security.*

1. Введение

Вопросы безопасности критических инфраструктур являются приоритетными в международной практике. Однако, каждой страной данный вопрос исследуется и прорабатывается индивидуально, исходя из категориальной сущности понятия «критиче-

ская инфраструктура» [1 – 3]. Тем не менее, функционально, общим для всех стран в данном вопросе являются значимость КИ на всех уровнях государств, ослабляющий социально-экономический эффект развития общества в случае нарушения работы КИ, сложность КИ по своей структуре. Кроме того, практически во всех странах используется секторальный подход к определению КИ и актуализируется проблема обеспечения безопасности КИ, в том числе, с учетом инфраструктурных зависимостей и связей. Анализ международного опыта построения и развития КИ показал эффективность рассмотрения КИ с точки зрения системного подхода, что выражается в представлении КИ на структурном, функциональном, макроскопическом и микроскопическом уровнях.

Уникальность РФ в решении данного вопроса определяется объектным построением и развитием КИИ на базе регулятивного подхода, в том числе, определяющегося в [4, 5]. Регулятивный подход, с одой стороны, создает «тепличные условия» для развития КИИ РФ, с другой стороны обладает существенным недостатком, определяемым на методологическом уровне, что предлагается устранить за счет введение «системного» взгляда на «обустройство» КИИ. Выявленные в ходе анализа функции инфраструктуры КИИ: структурная, дифференцирующая, коммуникационная, процессуальная, управленческая, регулятивные (концептуальные, проектные, плановые), являются основой становления и развития КИИ как системы.

Инфраструктурно, КИИ представляют собой взаимосвязанные системы, включающие субъекты и объекты КИИ. Так, в РФ субъекты КИИ (СКИИ) – собственники объектов КИИ (ОКИИ), функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. ОКИИ – информационные системы (ИС), автоматизированные системы управления (АСУ), информационно-телекоммуникационные системы (ИТС), подразделяются на значимые и не значимые [5]. Однако, вопрос обоснования учета информационного взаимодействия при разработке мер по обеспечению безопасности значимого ОКИИ пока не проработан. В решении данного вопроса, на наш взгляд, необходимо учесть:

– динамичность СКИИ на инфраструктурном уровне;

– обеспечение безопасного функционирования ОКИИ как целевой задачи в системе поддержки принятия решений по управлению эксплуатацией ОКИИ;

– увеличение значимости межобъектного взаимодействия при обеспечении безопасности КИИ на фоне отсутствия регулятивных методов и методик для их идентификации и оценки.

Таким образом, в качестве ключевой проблемы в процессе обеспечения безопасности КИИ, можно определить проблему, связанную с необходимостью учета факторов, связанных с инфраструктурной устойчивостью (ИУ) КИИ в процессе анализа ИБ и обеспечением возможности прогнозирования деструктивных воздействий (ДВ) при различных изменениях информационной инфраструктуры.

Оценка ИУ в настоящее время рассматривается как самостоятельная задача. Так, например, в работе [6] представлена схема обеспечения устойчивости функционирования КИИ в условиях угроз комплексных информационно-технических воздействий и информационно-психологических воздействий, приводящих к компьютерным инцидентам в КИИ. Вопросы зависимости устойчивости инфраструктуры от топологии рассмотрены в [7, 8]. Достаточно близким к понятию «устойчивость» является понятие «надежность», но она характеризуется обычно как мера вероятности устойчивой работы, вероятности безотказной работы [9].

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 и целостности рассматриваемой системы.

2. Используемые методы

КИИ является сложноструктурированной системой, для описания которой требуется учет большого количества факторов, что является определяющим для выбора метода нечеткого когнитивного анализа и сценарного моделирования [10-13] для ее исследования.

Применение когнитивного подхода в качестве основного инструмента моделирования задач управления и принятия решений в социальных и экономических системах обосновывается в работах А. Н. Целых, Л. А. Целых, Н. А. Абрамова, З. К. Авдеева, В. В. Борисов, В. Е. Гвоздев, Г.В. Горелова, Д.А. Новиков, Б. Г. Ильясов, В. А. Камаев, С. В. Ковриги, А. А. Кулинич, Д. Г. Лагерев, В. И. Максимов, Л. В. Массель, А. Г. Подвесовский, А. Н. Райков, В. Б. Силов, А. С. Федулов,R. Axelrod, P. P. Groumpos, B. Kosko, E .I. Papageorgiou, F.S. Roberts, J.L. Salmeron, C. D. Stylios, Y Y Haimes, P. Jiang. Однако в данных работах не рассматриваются вопросы управления ИБ инфраструктуры как сложной системы с учетом внутрисистемных деструктивно-образующих связей. При рассмотрении данного вопроса интересны работы Р. А. Демидова, П. Д. Зегжды, П. Ивановой, А. Е. Колоденковой, N. A. Jones, H. Ross, T. Lynam, P. Perez, A. Leitch, описывающие сложные информационные структуры, однако не исследующие вопросы комплексной обработки информации о состоянии инфор-

мационной инфраструктуры для поддержки принятия управленческих решений. Для инфраструктуры инфокоммуникационных систем с учетом факторов технического и экономического характера данные вопросы частично рассматривались в работах О. С. Лаута, Young-HyunChoi, S.Kukliński, Zhao, M. J. Creaner. Принципы функционирования и структура системы управления IT-инфраструктурой предложены Теленик С. Ф., Ролік О. І., Букасовым М. М., Соколовським Р. Л. Однако, ими не рассматривались аспекты ИБ.

Таким образом, вопрос оценки инфраструктурной устойчивости КИИ будем рассматривать с точки зрения комплексного учета различных факторов инфраструктурного, технического, экономического и регулятивного характера для поддержки принятия решений во время управления ИБ КИИ.

3. Дискуссия

Оценка ИУ КИИ выполнялась в рамках комплексной оценки ИБ КИИ для реализации которой разработана соответствующая когнитивная модель, где кроме регулятивных составляющих, регламентированных в документе [5], предусматривается влияние на целевой концепт факторов, связанных с деструктивными воздействиями инфраструктурного характера (рисунок 1).

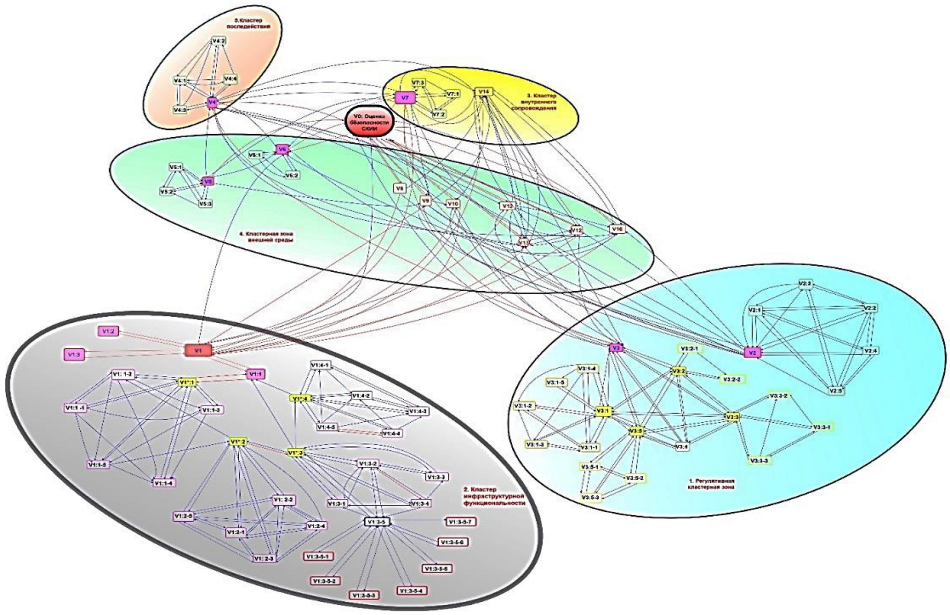

Рис. 1. Когнитивная модель «Оценка информационной безопасности КИИ при деструктивных воздействиях»

Представленная на рисунке 1 когнитивная модель имеет многоуровневую структуру. К примеру, для оценки инфраструктурного деструктивизма, в том числе определены концепты: V1*:1 «Ошибки, связанные с развитием СЗИ СКИИ на разных этапах жизненного цикла», V1*:2 «Оценка факторов риска безопасности СКИИ инфраструктурного характер», V1*:4 «Оценка факторов риска безопасности СКИИ, связанных с межсубъектными связями», представленные на втором уровне модели. К концептам третьего уровня модели отнесены, к примеру, V1:1-3 «Ошибки при реализации системы защиты субъекта КИИ», V1:1-5 «Отсутствие (не корректное построение) системы разграничения доступа в среде субъекта КИИ», V1:3-2 «Не учет межобъектных связей в среде субъекта КИИ», V1:3-5 «Наличие деструктивно-образующих межобъектных связей», V1:4-1 «Не учет межсубъектных отношений в среде функционирования КИИ», V1:4-2 «Снижение уровня безопасности хотя бы одного из взаимодействующих субъектов КИИ» и др. [16].

Инфраструктурная устойчивость СКИИ проявляется в инертной форме и в контексте когнитивного моделирования ИБ СКИИ может рассматриваться как мера силы концепта V1: «Оценка функциональности СКИИ» [14, 15]. При этом, в рамках когнитивного моделирования, традиционно, значения концептов задаются экспертно. В это же время, на наш взгляд, возможна ее оценка с использованием аппарата логико-вероятностного моделирования, путем четкой структуризации системы – СКИИ. Таким образом, повышается уровень достоверности получаемых результатов.

В ходе исследования инфраструктурной устойчивости СКИИ предлагается выполнить процедуру структуризации СКИИ как системы через процедуру деструктуризации инфраструктуры соответствующего субъекта и определения топологических особенностей полученных подсистем. Согласно [16] при декомпозиции структуры СКИИ можно выделить односвязную, многосвязную, логическую декомпозиции структуры, а также декомпозицию, связанную с разложени-

ем по полной группе событий относительно выделенных элементов, блоков и др. Применительно к КИИ возможны также декомпозиции системы на уровне КИИ (для межсубъектного взаимодействия) и на уровне СКИИ (для межобъектного взаимодействия).

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.

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.

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.

С этой точки зрения необходимо в структуре СКИИ выделить 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 подъобъектов КИИ и других характеристик инфраструктурной устойчивости целесообразно воспользоваться структурно-логическими схемами надежности, в которых учитываются взаимосвязь элементов друг с другом и их влияние на работоспособность СКИИ как системы.

Оценка инфраструктурной устойчивости СКИИ P_{subj} рассчитывается аналогично схемам оценки инфраструктурной устойчивости ОКИИ для параллельного и последовательного соединения ОКИИ. Далее, для оценки инфраструктурной устойчивости СКИИ осуществляется формирование структурной схемы взаимосвязи ОКИИ и, исходя из вероятностей безотказной работы ОКИИ и вероятности реализации угроз, рассчитывается оценка инфраструктурной устойчивости СКИИ.

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

Оценка инфраструктурной устойчивости СКИИ на уровне инфраструктуры субъекта в когнитивной модели «Оценка ИБ СКИИ» реализована на уровне подсистем. Результаты работы данной модели представлены:

1) оценкой коэффициента инфраструктурной целостности СКИИ (как исходного данного для оценки силы концепта V1 «Оценка функциональности СКИИ») – K(inf_int);

2) оценкой коэффициента структурной функциональности СКИИ (как исходного данного для оценки силы концепта V1 «Оценка функциональности субъекта КИИ») – K(str_func);

3) набором сценариев достижения требуемого уровня функциональности СКИИ в зависимости от вида инфраструктуры СКИИ.

Оценку коэффициента инфраструктурной целостности СКИИ K(inf_int) предложено выполнить с учетом топологии подсистемы взаимодействующих ОКИИ. Данный показатель напрямую определяется целостностью подсистем взаимодействующих объектов (ПВО) СКИИ.

Оценка целостности ПВО СКИИ выполняется исходя из реализации комплекса мероприятий, связанных с оценкой прогнозируемых состояний информационной инфраструктуры на соответствие предъявляемым требованиям и регламентам. Структурные характеристики системы в данном случае являются показателями качества инфраструктуры с точки зрения системного подхода.

Кроме того, вводим новый показатель – коэффициент структурной функциональности СКИИ – K(str_func). Данный показатель не является стандартной топологической характеристикой с точки зрения системного подхода и теории надежности систем. В данном исследовании он введен для определения значения соответствующего концепта.

Для оценки K(str_func) разработана модель оценки коэффициента инфраструктурной функциональности СКИИ. Алгоритмически, она представлена следующим набором шагов:

Шаг 1: анализ инфраструктуры СКИИ.

Шаг 2: декомпозиция инфраструктуры СКИИ путем выделения подсистемы взаимодействующих объектов.

Шаг 3: построение модели «Оценка структурной

функциональности СКИИ» в виде инфраструктурной схемы взаимодействующих объектов. Для данной модели:

1) веса связей O_{ij} определяются экспертным путем, исходя из вида взаимосвязи,

2) значения концептов F(Oi) устанавливаются, исходя из категорий значимости соответствующих объектов в шкале [0,1] по заданному правилу,

3) значения весов связей «Oi_F(Sj)» равны +1 для всех i, j,

4) значения весов связей «F(Sj)_V1» равны +1 для всех j.

Шаг 4: На основе треугольной функции принадлежности оцениваем значение коэффициента структурной функциональности K(str_func).

4. Экспериментальное исследование

Предложенная модель оценки ИУ КИИ в рамках комплексной оценки ИБ КИИ имеет программную реализацию (рисунок 2) [17 – 25], для разработки которых в том числе использовалась [26, 27] и апробирована в ходе экспериментального исследования на базе СКИИ Поликлиника.

В соответствии с договором на НИР было произведено обследование технических средств Поликли-

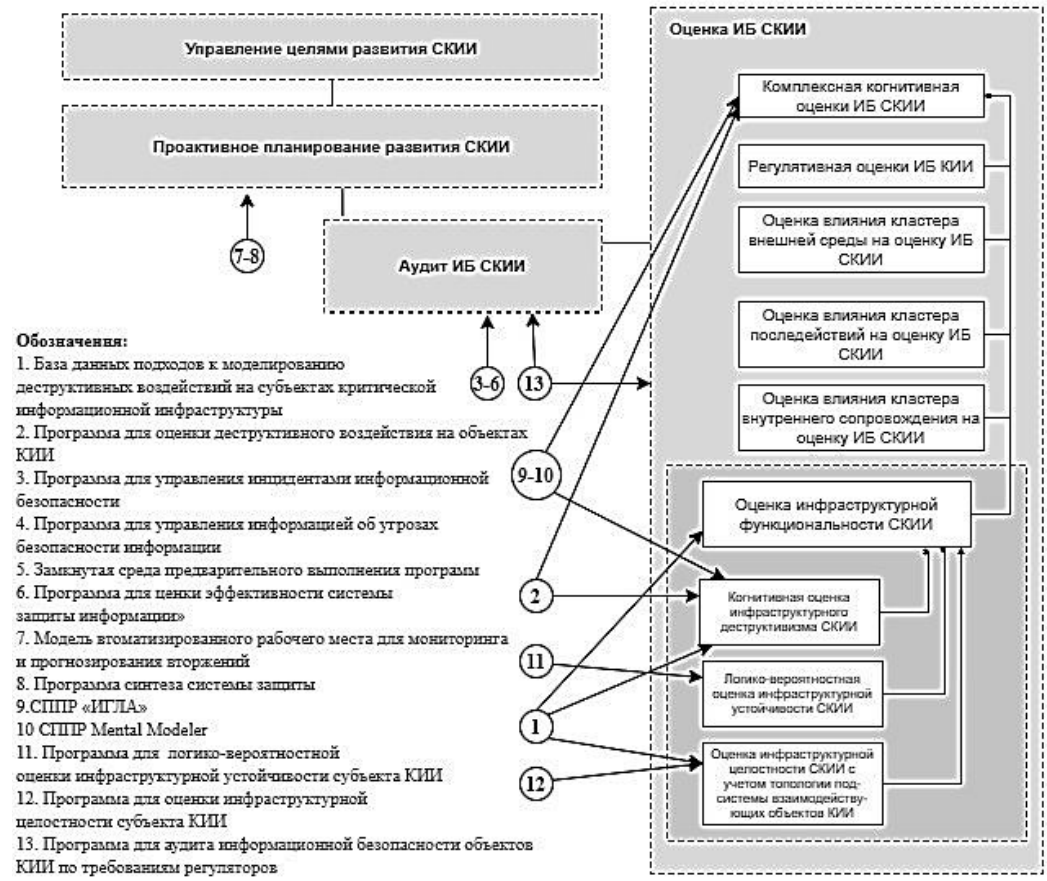

Рис. 2. Систематизация использования программных средств при решении задачи обеспечения безопасности СКИИ при ДВ

ники по требованиям регуляторов. В результате обследования было выявлено, что на данных технических средствах ведется обработка персональных данных работников и пациентов Поликлиники. Технические средства объединены в локальную сеть. Локальная сеть в Поликлинике является одноранговой, имеющей подключение к сетям связи общего пользования.

На момент обследования была представлена информация о следующих ИС, в которых обрабатываются персональные данные в Поликлинике – O_1: ИСПДн «1С зарплата и кадры»; O_2: ИСПДн «1С Бухгалтерия»; O_3: ИСПДн «Система видеонаблюдения»; O_4: ИС «Система пожарной охраны»; O_5: ИСПДн МИС «Инфоклиника»; O_6: ИСПДн МИС «1С ОМС»; O_7: ИСПДн «База данных «Chip»»; O_8: ИСПДн «МИС ПАКС».

Согласно [5] определены категории значимости ОКИИ: $Cat\_Zn(O_1) \equiv 3$, $Cat\_Zn(O_2) \equiv 3$, $Cat\_Zn(O_3) \equiv O3$; $Cat\_Zn(O_4) \equiv 3$, $Cat\_Zn(O_5) \equiv 2$, $Cat\_Zn(O_6) \equiv 3$, $Cat\_Zn(O_7) \equiv 3$, $Cat\_Zn(O_8) \equiv 3$.

Исходя из анализа исходных данных, полученных при анкетировании работников Поликлиники, все ИСПДн были объединены в две группы:

– подсистема S1: «не медицинская» – ИСПДн «Бухгалтерия, кадры и системы сопровождения». Работники подсистемы S2 осуществляют передачу данных в сторонние организации;

– подсистема S2: «медицинская» – ИСПДн «Пациенты». Работники ИСПДн «Пациенты» осуществляют передачу данных в Территориальный фонд медицинского страхования региона, региональный областной медицинский информационно-аналитический центр и комитет здравоохранения области, используя ПО ViPNet Client 4.x (сеть Интернет) и АПКШ «континент-К» (защищенная сеть передачи данных «РИСЗ»).

В результате обследования ИС Поликлиники выявлены реализуемые меры по защите информации на объектах КИИ.

В ходе исследования выполнялись следующие виды работ: 1) сбор сведений о программном обеспечении, установленном на ПК; 2) сбор сведений об аппаратном обеспечении и его характеристик; 3) опрос пользователей, с целью выявления уязвимых мест защиты информации, обрабатываемой на данном ПК; 4) сбор и анализ данных о физической защите информации.

В ходе аудита ИБ Поликлиники стандартными методами, оценка ИБ определена на среднем уровне, с выдачей соответствующих рекомендаций по ее повышению.

На следующем этапе исследование выполнялось с использованием представленных методов и моделей. Для этого:

Шаг 1. Выполнена декомпозиция инфраструктуры Поликлиники на подсистемы взаимодействующих объектов (рисунок 3).

По результатам данного этапа определено следующее:

1) в составе СКИИ Поликлиника – 2 подсистемы

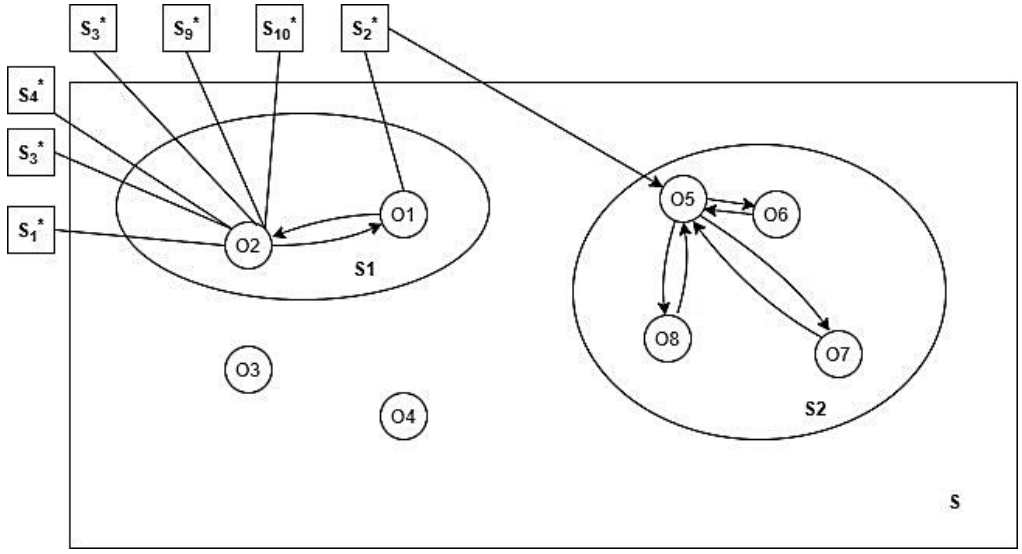

Рис. 3. Декомпозиция инфраструктуры СКИИ Поликлиника на подсистемы взаимодействующих объектов

взаимодействующих объектов и два локальных ОКИИ, не участвующих во взаимодействии ни на внутреннем, ни на внешнем уровнях;

2) объект О1 имеет двустороннюю связь с внешним СКИИ S_2*;

3) объект О2 имеет двустороннюю связь с внешними СКИИ S_1*, S_3*– S_7*;

4) существует односторонняя связь между S_2* и O_5;

5) двусторонние связи присутствуют между объектами: О1 и О2, О5 и О6, О5 и О7, О5 и О8.

Шаг 2. Определено наличие возможных деструктивных межсубъектных взаимодействий.

В ходе анализа определено наличие межсубъектных взаимодействий по сферам: здравоохранение (Z), банковская и иная финансовая сфера (B): «Z – Z», «Z – B», «B – Z». Где:

1) межсубъектное взаимодействие вида «Z – B» является нейтральным;

2) межсубъектное взаимодействие вида «B – Z» является косвенным, т. е. изменение состояния СКИИ из банковской сферы может повлечь за собой изменения в состоянии СКИИ сферы здравоохранения при выполнении определенного рода условий;

3) межсубъектное взаимодействие вида «Z – Z» может рассматриваться как деструктивно-образующее, так как изменение состояния одного субъекта приводит к изменениям в состоянии другого субъекта.

Таким образом приходим к следующему выводу.

Вывод: для предотвращения ИД на уровне межсубъектного взаимодействия рекомендуется использовать дополнительные средства защиты в системах взаимодействия: во-первых, в ИС ТФОМС с ИСПДн «1С Бухгалтерия» Поликлиники; во-вторых, в ИС ОМИ-

АЦ с ИСПДн «1С Бухгалтерия», ИСПДн «1С зарплата и кадры», ИСПДн МИС «Инфоклиника» Поликлиники.

Шаг 3. Откорректированы категории значимости ОКИИ СКИИ Поликлиники.

Для выполнения данного шага определены подсистемы взаимодействующих объектов, в которых категории значимости имеют различные значения. Так, в подсистеме S_2 объекту O_5 присвоена вторая категория значимости, категория значимости взаимодействующих с данным объектов O_6, O_7 и O_8 – третья.

Важно отметить, что в данной подсистеме присутствуют двусторонние связи между объектами O_5 и O_6, O_5 и O_7, O_5 и O_8. Таким образом, возникает вопрос о необходимости корректировки категорий значимости объектов O_6, O_7 и O_8, так как они имеют категорию значимости ниже, чем у взаимодействующего с ними объекта O_5. Данные ОКИИ представляют из себя ИС. По результатам экспертного опроса определены виды межобъектных взаимодействий, согласно чего можно говорить об отсутствии необходимости корректировки категорий значимости ОКИИ Поликлиники.

Шаг 4. Выполнена оценка ИЦ СКИИ Поликлиника.

Шаг 4.1. Выполнена оценка топологических показателей.

Для оценки ИЦ СКИИ Поликлиника использована программа для оценки ИЦ СКИИ [26]. По результатам работы получены оценочные данные (таблица 1).

По результатам анализа матрицы связности констатируем наличие в структуре СКИИ обрывов и висячих вершин. Кроме того, параметр R, отвечающий за структурную избыточность меньше нуля, что говорит об отсутствии связанности инфраструктуры на данном СКИИ. По параметрам структурной компактности данный субъект не является относительно целостным, так как соответствующий параметр Qотн <0. По оценке степени централизации: так как $\sigma \neq 1$ и $\sigma \neq 0$, то можно говорить о том, что исследуемый СКИИ не относится к типам: звезда, полный граф и кольцо.

Таблица 1

Количественные значения показателей ИЦ СКИИ Поликлиника

Показатель ИЦ	Количественное значение
Структурная избыточность, R	– 0.765
Неравномерность распределения связей, ε^2 (для систем с большой избыточностью)	– 8.22
Абсолютная компактность, Q	36
Относительная компактность, Qотн	– 0.88
Диаметр, d	2
Индекс центральности, σ	None

Шаг 4.2. Выполнена оценка коэффициента структурной функциональности СКИИ Поликлиника.

Для оценки коэффициента структурной функциональности СКИИ Поликлиника построен вероятностный граф межобъектного влияния (рисунок 4).

Для определения K(str_func) использована шкала соответствия значений концептов и категорий значимости ОКИИ, согласно которой: $Cat\_Zn(Oi) \equiv 3$, $i = \{1, 2, 3, 4, 6, 7, 8\} \Longrightarrow F\_zn(Oi) \equiv 0{,}35$, $Cat\_Zn(O5) \equiv 2 \Longrightarrow F\_zn(O5) \equiv 0{,}7$.

По результатам экспертной оценки определены значения МОС (таблица 2).

В итоге, получено рассчитанное значение K(str_func) = 2,52; (Max_K(str_func) = 4.85) (таблица 3). Данное значение определяет значение концепта «Оценка ИЦ СКИИ» в общей когнитивной модели «Прогнозирование развития ситуаций и оценка ИБ СКИИ при деструктивных воздействиях».

Шаг 5. Выполнена оценка ИУ СКИИ Поликлиника.

Оценка ИУ СКИИ Поликлиника выполнено с помощью обозначенного выше алгоритма. В результате, значение ИУ получено на уровне 0.14.

По имеющимся исходным данным с помощью разработанного программного средства выполнено построение схемы взаимодействия подобъектов ОКИИ Поликлиники (рисунок 5).

Для оценки ИУ СКИИ использовались значения вероятностей реализации угроз, спрогнозированные на основе существующей статистики компании InfoWatch по инцидентам ИБ на предприятиях и в организациях, функционирующих в сферах КИИ [29]. Оценка ИУ СКИИ Поликлиника показала недостаточный уровень ИУ.

В данной ситуации возможно два варианта дальнейших действий: 1) полученный результат использовать для оценки ИБ СКИИ. В данном случае полученное значение будет принято, как значение соответствующего концепта; 2) воспользоваться предлагаемыми рекомендациями.

Шаг 6. Выполнена оценка и исследован ИД СКИИ Поликлиника.

Шаг 6.1. Статичный анализ.

В ходе работы с разработанной когнитивной моделью (рисунок 6), тип вершин V1*:1 и V1*:4 определен как «управляемый», с целью сокращения затрачиваемых вычислительных мощностей.

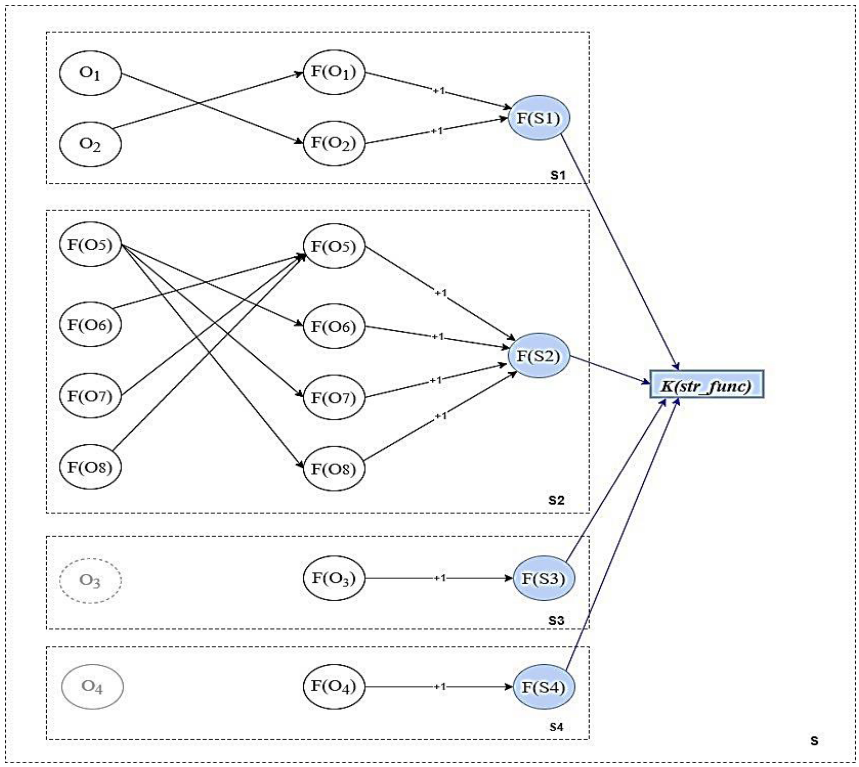

Рис. 4. Модель «Оценка коэффициента структурной функциональности СКИИ Поликлиника»

Таблица 2

Матрица значений МОС на СКИИ Поликлиника

	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8
O_1	0	0.5	0	0	0	0	0	0
O_2	0.5	0	0	0	0	0	0	0
O_3	0	0	0	0	0	0	0	0
O_4	0	0	0	0	0	0	0	0
O_5	0	0	0	0	0	0.7	0.8	0.2
O_6	0	0	0	0	0.3	0	0	0
O_7	0	0	0	0	0.6	0	0	0
O_8	0	0	0	0	0.1	0	0	0

Таблица 3

Расчётные значения для оценки коэффициента структурной функциональности СКИИ Поликлиника

Sj	Oi	Cat_Zn(Oi)	F_zn(Oi)	F(Oi)	max F(Oi)	Cat_Zn(Sj)	F_ zn(Sj)	F(Sj)	max F_zn(Sj)
S_1	O_1	3	0.35	0.175	0.5	3	0.35	0.35	1
	O_2	3	0.35	0.175	0.5				
S_2	O_5	2	0.7	0.35	1.05	2	0.7	1.47	3.15
	O_6	3	0.35	0.49	0.7				
	O_7	3	0.35	0.56	0.7				
	O_8	3	0.35	0.07	0.7				
S_3	O_3	3	0.35	0	0	3	0.1	0.35	0.35
S_4	O_4	3	0.35	0	0	3	0.35	0.35	0.35

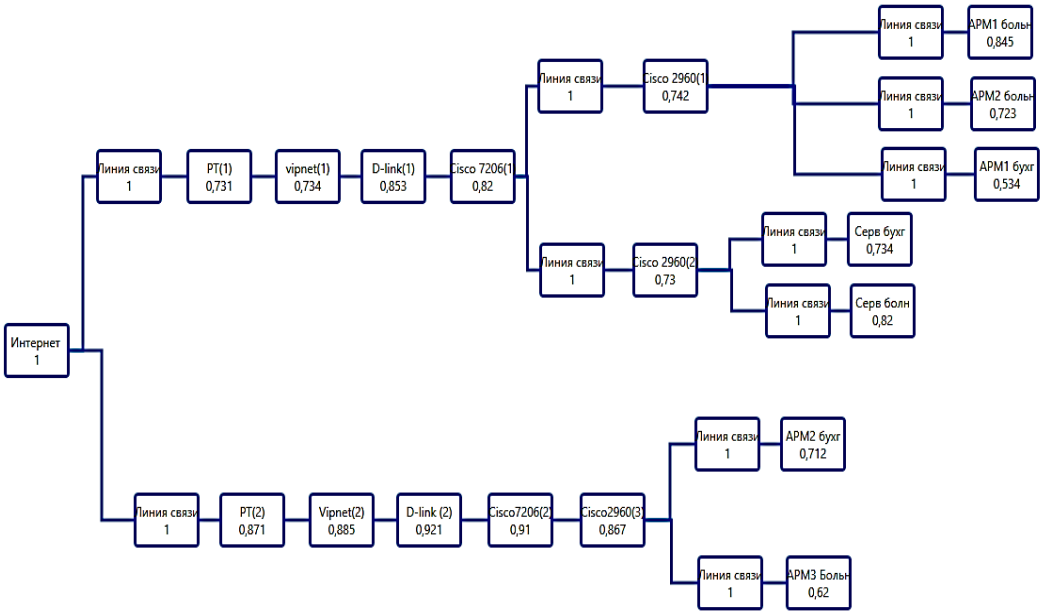

Рис. 5. Схема взаимодействия подобъектов ОКИИ Поликлиника на примере ИСПДн МИС «Инфоклиника»

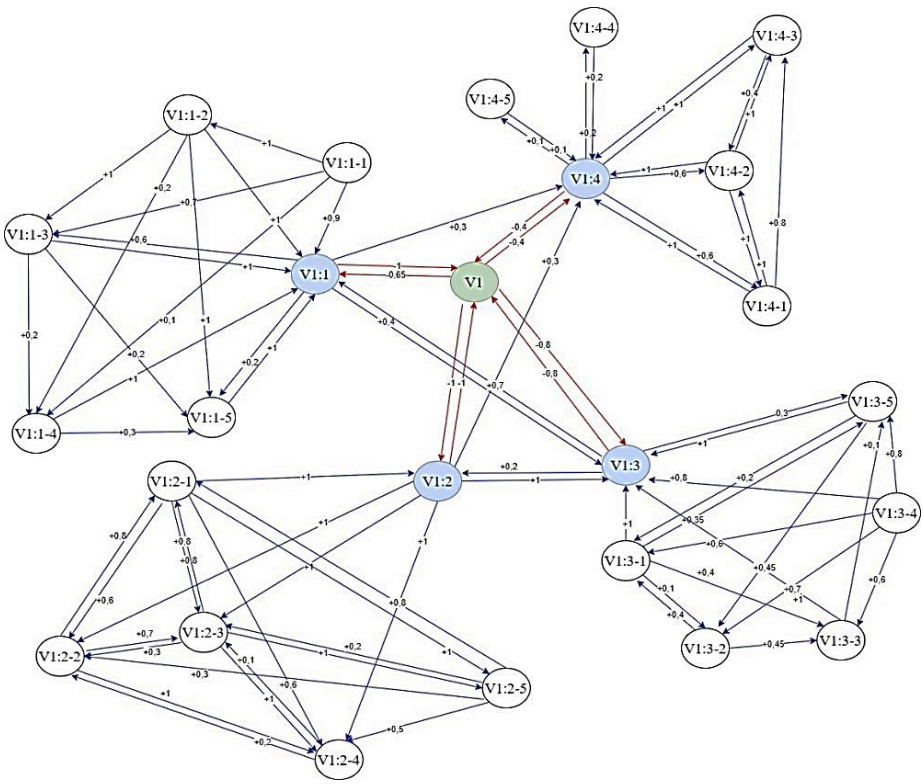

Рис. 6. Когнитивная модель «Оценка ИД СКИИ Поликлиника»

Таким образом, исходная когнитивная модель отождествляется с вариантом когнитивной модели, в которой, в отличии от рассматриваемой, поведение концептов третьего уровня, влияющих на концепты V1*:1 и V1*:4 в явном виде не рассматривается. В качестве целевых определены вершины V1 и V1*:2.

В ходе исследования по результатам экспертной оценки построена матрица взаимного влияния факторов когнитивной модели «Оценка ИД СКИИ Поликлиника» и рассчитаны значения системных показателей когнитивной модели «Оценка функциональности СКИИ».

Расчет системных показателей построенной когнитивной карты выявил высокий уровень консонан-

са. Оцененные консонансные значения концептов принимают максимальные значения, что говорит о высокой степени доверия к разработанной модели.

Анализ полученных значений позволяет определить концепты, оказывающие наиболее сильное влияние на систему. Так, наиболее сильное положительное влияние на систему среди всех концептов оказывают концепты: «Ошибки, связанные с первичной разработкой информационной инфраструктуры организации (предприятия)» (V1:1-1); «Инфраструктурное возмущение системы» (V1:3-4); «Ошибки инфраструктурного анализа» (V1:3-1); «Инфраструктурные ошибки при развитии СКИИ» (V1:2); «Ошибки при сопровождении СКИИ» (V1:2-1); «Реализация атаки на ОКИИ» (V1:2-2); «Ошибки при анализе требований для СКИИ» (V1:2-3); «Ошибки, связанные с определением перечня объектов, подлежащих категорированию» (V1:2-4). Соответствующие значения: 0.2584, 0.2525, 0.2493, 0.2460, 0.2460, 0.2460, 0.2460, 0.2460 соответственно (рисунок 7).

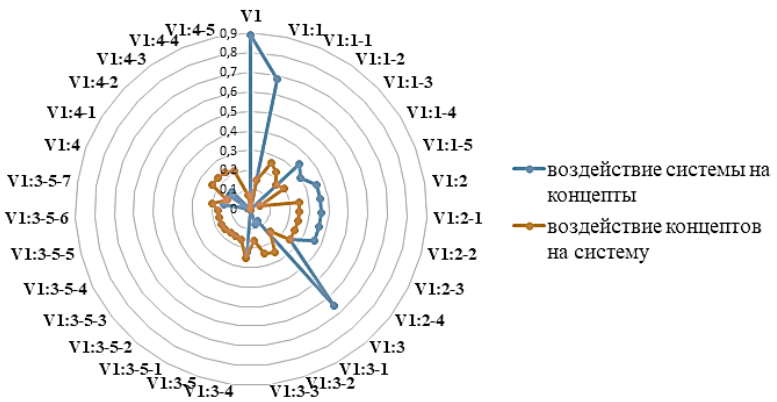

Рис. 7. Диаграмма результатов элементов статического анализа когнитивной модели «Оценка ИД СКИИ Поликлиника»

Отрицательно влияя на вышеперечисленные факторы, можно «сдвинуть» всю систему в положительную сторону. «Отрицательно» – в связи с формулировкой концептов.

Таким образом, с помощью когнитивного анализа выполнена формулировка концептов, которые наиболее сильно влияют на оценку функциональности СКИИ: ошибки, связанные с первичной разработкой информационной инфраструктуры Поликлиники, инфраструктурное возмущение системы, ошибки инфраструктурного анализа, инфраструктурные ошибки при развитии СКИИ, ошибки при сопровождении СКИИ, реализация атаки на ОКИИ, ошибки при анализе требований для СКИИ. Воздействуя на вышеперечисленные факторы, можно значительно повысить уровень безопасности СКИИ.

Результаты

Отличительной особенностью предложенного метода оценки ИУ СКИИ является системный подход к новому объекту защиты – СКИИ, а также комплексный подход к оценке ИБ. Для оценки ИБ, помимо регулятивных составляющих, предложено учитывать инфраструктурные особенности субъекта, порождающие угрозу саморазрушения системы. Основой алгоритма прогнозирования развития ситуаций и оценки ИБ СКИИ при деструктивных воздействиях являются сформулированные принципы выполнения декомпозиции СКИИ на подсистемы взаимодействующих объектов. Экспериментально подтверждено, что выделенные виды деструктивных воздействий инфраструктурного характера оказывают влияние на оценку ИБ СКИИ, что дает дополнительную информацию для принятия управленческих решений по вопросам обеспечения безопасности КИИ.

Литература

1. Infrastructure for the 21st Century Framework for a Research Age. [Электронный ресурс] / Vining Aidan R., Richards John (eds.). – Режим доступа: http://www.noravank.am/upload/pdf/21_VEK_01_2018.pdf.

2. Infrastructure Capital: What Is It? Where Is It? How Much of It Is There? [Электронный ресурс] / J. R. Baldwin, J. Dixon. – Режим доступа: https://www.researchgate.net/publication/23649155_Infrastructure_Capital_What_Is_It_Where_Is_It_How_Much_of_It_Is_There.

3. О критических инфраструктурах Евразийской интеграции [Электронный ресурс] / Г. Арутюнян. – Режим доступа: www.noravank.am/ rus/issues/detail.php?ELEMENT_ID=16344.

4. О безопасности критической информационной инфраструктуры Российской Федерации: Фе-

деральный закон от 26 июля 2017г. N 187-ФЗ (с изм. и доп.) [Электронный источник]. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

5. 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: Постанов Постановление Правительства РФ от 8 февраля 2018 г. № 127 (не вступил в силу) [Электронный источник]. – URL: https://www.garant.ru/products/ipo/prime/doc/71776120/.

6. 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.

7. Гаджиев Б.Р., Гибина Е.Ю., Прогулова Т.Б., Щетинина Д.П. Топология и устойчивость локально-мировых сетей // Программные продукты и системы № 4, 2009. С.51-54 - URL: https:// topologiya-i-ustoychivost-lokalno-mirovyh-setey.pdf.

8. 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.

9. Косолапов О.В. Устойчивость как одна из основных характеристик системы [Электронный ресурс] / О.В. Косолапов, М.Н. Игнатьева. // Известия Уральского государственного горного университета. — Электрон. дан. — 2013. — № 4. — С. 77-81. — URL: https://e.lanbook.com/journal/issue/290438. — Загл. с экрана.

10. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам: пер. с англ. М.: Наука, 1986. 496 с

11. Kosko V. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. 1986. Vol. 24. P. 65–75.

12. Ажмухамедов И.М. Информационная безопасность. Системный анализ и нечеткое когнитивное моделирование. – М.: Изд-во LAP, 2012. –385с.

13. Садовникова Н. П. Выбор стратегий территориального развития на основе когнитивного анализа и сценарного моделирования [Электронный ресурс] / Н. П. Садовникова, Н. П. Жидкова // Интернет-вестник ВолгГАСУ : серия Строительная информатика. - 2012. - № 7 (21). – URL: http://vestnik.vgasu.ru/attachments/SadovnikovaZhidkova-2012_7(21).pdf.

15. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103

16. 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.

17. Викторова В. С., Степанянц А. С. Многоуровневое моделирование надежности систем // Датчики и системы. – 2014. – № 6(181). – С. 33–37.

18. Патент на полезную модель № 139517 U1 Российская Федерация, МПК G06F 17/10. Автоматизированное рабочее место для мониторинга и прогнозирования вторжений / В. А. Корнева, Е. А. Максимова; заявитель Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Волгоградский государственный университет». – № 2013133255/08: заявл. 16. 07. 2013: опубл. 20.04.2014. – 2 с.

19. Патент на полезную модель №139517. Российская Федерация, Автоматизированное рабочее место для мониторинга и прогнозирования вторжений / В. А. Корнева, Е. А. Максимова; патентообладатель ФГАОУ ВО ВолГУ. – №2013133255; приоритет от 16.07.2013., зарегистр.19.03.2014, Бюл. № 11. – 2 с.

20. Свидетельство о государственной регистрации программы для ЭВМ №2020667300. Российская Федерация. Оценка деструктивного воздействия на объектах критической информационной инфраструктуры / Е. А. Максимова, М. Е. Каменнов; правообладатель ФГАОУ ВО ВолГУ. – №2020662052; заявл. 12.10.2020; опублик. 22. 12. 2020 – 1 с.

21. Свидетельство о регистрации программы для ЭВМ № 2021610425. Российская Федерация. Средство управления инцидентами информационной безопасности “ВЕКТОР” / М. Е. Каменнов, Е. А. Максимова, Ю. Н. Голубев; правообладатель ООО «Региональный аттестационный центр». – № 2020667689, заявл. 28.12.2020; опублик. 14.01.2021 – 1 с.

22. Свидетельство о регистрации программы для ЭВМ № 2021610482. Российская Федерация. Средство управления информацией об угрозах безопасности информации “БЕРЕСТЬЕ”/ М. Е. Каменнов, Е. А. Максимова, Ю. Н .Голубев; правообладатель ООО «Региональный аттестационный центр», № 2020667772, заявл. 28.12.2020; опублик. 14.01.2021 – 1 с.

23. Свидетельство о государственной регистрации программы для ЭВМ № 2019660368 Россий-

ская Федерация. Замкнутая среда предварительного выполнения программ «ТОР»/ В. А. Петров, Е. А. Максимова, Ю. Н. Голубев, М. В. Пономарев; заявитель Общество с ограниченной ответственностью «Региональный аттестационный центр». – № 2019619100: заявл. 24. 07. 2019: опубл. 05. 08. 2019 – 1 с.

24. Свидетельство о государственной регистрации программы для ЭВМ №2015662413. Российская Федерация. Оценка эффективности системы защиты информации / А. В. Петькиев, Е. А. Максимова; правообладатель ФГАОУ ВО ВолГУ. – №2015619218, заявл. 05. 10. 2015 г.; опублик. 24. 11. 2015. – 1 с.

25. Свидетельство о государственной регистрации программы для ЭВМ №2012618761. Российская Федерация. Синтез системы защиты / Максимова, В. А. Корнева; правообладатель ФГАОУ ВО ВолГУ. – № 2012616588; заявл. 01. 08. 2012; опублик. 26. 09. 2021. – 1 с.

26. Свидетельство о государственной регистрации программы для ЭВМ № 20216666613 Российская Федерация. Оценка инфраструктурной целостности субъекта критической информационной инфраструктуры / Е. А. Максимова; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Волгоградский государственный университет». – № 2021665746: заявл. 12. 10. 2021: опубл. 18. 10. 2021 – 1 с.

27. MentalModeler [Электронный ресурс]: сайт. – Режим доступа: http://www.mentalmodeler.org/

28. СППР «ИГЛА» [Электронный ресурс]: сайт. – Режим доступа: http://iipo.tu-bryansk.ru/quill/download.html.

29. Аналитика отрасли информационной безопасности [Электронный ресурс]: сайт. – Режим доступа: https://www.infowatch.ru/analytics/analitika.

References

1. Infrastructure for the 21st Century Framework for a Research Age. [Электронный ресурс] / Vining Aidan R., Richards John (eds.). – Режим доступа: http://www.noravank.am/upload/pdf/21_VEK_01_2018.pdf.

2. Infrastructure Capital: What Is It? Where Is It? How Much of It Is There? [Электронный ресурс] / J. R. Baldwin, J. Dixon. – Режим доступа: https://www.researchgate.net/publication/23649155_Infrastructure_Capital_What_Is_It_Where_Is_It_How_Much_of_It_Is_There.

3. O kriticheskikh infrastrukturakh Yevraziyskoy integratsii [Elektronnyy resurs] / G. Arutyunyan. – Rezhim dostupa: www.noravank.am/ rus/issues/detail.php?ELEMENT_ID=16344.

4. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Federal'nyy zakon ot 26 iyulya 2017g. N 187-FZ (s izm. i dop.) [Elektronnyy istochnik]. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

5. Ob utverzhdenii Pravil kategorirovaniya ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe Perechnya pokazateley kriteriyev znachimosti ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy: Postanov Postanovleniye Pravitel'stva RF ot 8 fevralya 2018 g. № 127 (ne vstupil v silu) [Elektronnyy istochnik]. – URL: https://www.garant.ru/products/ipo/prime/doc/71776120/.

6. 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 // Voprosy kiberbezopasnosti. 2019. № 6(34), s .37–48.

7. Gadzhiyev B.R., Gibina Ye.YU., Progulova T.B., Shchetinina D.P. Topologiya i ustoychivost' lokal'no-mirovykh setey // Programmnyye produkty i sistemy № 4, 2009. C.51-54 - URL: https:// topologiya-i-ustoychivost-lokalno-mirovyh-setey.pdf.

8. Balashova T.I. obespecheniye otkazoustoychivosti seti povysheniyem nadezhnosti yeyo topologii // Sovremennyye problemy nauki i obrazovaniya. – 2014. – № 6. - URL: http://science-education.ru/ru/article/view?id=16846.

9. Kosolapov O.V. Ustoychivost' kak odna iz osnovnykh kharakteristik sistemy [Elektronnyy resurs] / O.V. Kosolapov, M.N. Ignat'yeva. // Izvestiya Ural'skogo gosudarstvennogo gornogo universiteta. — Elektron. dan. — 2013. — № 4. — C. 77-81. — URL: https://e.lanbook.com/journal/issue/290438. — Загл. с экрана.

10. Robertc F.S. Diskretnyye matematicheskiye modeli s prilozheniyami k sotsial'nym, biologicheskim i ekologicheskim zadacham: per. s angl. M.: Nauka, 1986. 496 c

11. Kosko V. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. 1986. Vol. 24. P. 65–75.

12. Azhmukhamedov I.M. Informatsionnaya bezopasnost'. Sistemnyy analiz i nechetkoye kognitivnoye modelirovaniye. – M.: Izd-vo LAP, 2012. -385c.

13. Sadovnikova N. P. Vybor strategiy territorial'nogo razvitiya na osnove kognitivnogo analiza i stsenarnogo modelirovaniya [Elektronnyy resurs] / N. P. Sadovnikova, N. P. Zhidkova // Internet-vestnik VolgGASU: seriya Stroitel'naya informatika. - 2012. - № 7 (21). – URL: http://vestnik.vgasu.ru/attachments/SadovnikovaZhidkova-2012_7(21).pdf.

15. Maksimova Ye.A. Kognitivnoye modelirovaniye destruktivnykh zloumyshlennykh vozdeystviy na ob"yektakh kriticheskoy informatsionnoy infrastruktury // Trudy uchebnykh zavedeniy svyazi. 2020. T. 6. № 4. C. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103

16. Maksimova Ye.A. Otsenka informatsionnoy bezopasnosti sub"yekta kriticheskoy informatsionnoy infrastruktury pri destruktivnykh vozdeystviyakh//Monografiya: Feder. gos. avt. obrazovat. uchrezhdeniye vyssh. obrazovaniya «Volgogr. gos. un-t»». - Volgograd: Izd-vo VolGU, 2020.- 95 c.

17. Viktorova V. S., Stepanyants A. S. Mnogourovnevoye modelirovaniye nadezhnosti sistem // Datchiki i sistemy. – 2014. – № 6(181). – C. 33-37.

18. Patent na poleznuyu model' № 139517 U1 Rossiyskaya Federatsiya, MPK G06F 17/10. Avtomatizirovannoye rabocheye mesto dlya monitoringa i prognozirovaniya vtorzheniy / V. A. Korneva, Ye. A. Maksimova; zayavitel' Federal'noye gosudarstvennoye avtonomnoye obrazovatel'noye uchrezhdeniye vysshego professional'nogo obrazovaniya "Volgogradskiy gosudarstvennyy universitet". – № 2013133255/08: zayavl. 16. 07. 2013: opubl. 20.04.2014. – 2 c.

19. Patent na poleznuyu model' №139517. Rossiyskaya Federatsiya, Avtomatizirovannoye rabocheye mesto dlya monitoringa i prognozirovaniya vtorzheniy / V. A. Korneva, Ye. A. Maksimova; patentoobladatel' FGAOU VO VolGU. – №2013133255; prioritet ot 16.07.2013., zaregistr.19.03.2014, Byul. № 11. – 2 c.

20. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2020667300. Rossiyskaya Federatsiya. Otsenka destruktivnogo vozdeystviya na ob"yektakh kriticheskoy informatsionnoy infrastruktury / Ye. A. Maksimova, M. Ye. Kamennov; pravoobladatel' FGAOU VO VolGU. – №2020662052; zayavl. 12.10.2020; opublik. 22. 12. 2020 – 1 c.

21. Svidetel'stvo o registratsii programmy dlya EVM № 2021610425. Rossiyskaya Federatsiya. Sredstvo upravleniya intsidentami informatsionnoy bezopasnosti "VEKTOR" / M. Ye. Kamennov, Ye. A. Maksimova, YU. N. Golubev; pravoobladatel' OOO «Regional'nyy attestatsionnyy tsentr». – № 2020667689, zayavl. 28.12.2020; opublik. 14.01.2021 – 1 c.

22. Svidetel'stvo o registratsii programmy dlya EVM № 2021610482. Rossiyskaya Federatsiya. Sredstvo upravleniya informatsiyey ob ugrozakh bezopasnosti informatsii "BEREST'Ye"/ M. Ye. Kamennov, Ye. A. Maksimova, YU. N. Golubev; pravoobladatel' OOO «Regional'nyy attestatsionnyy tsentr», № 2020667772, zayavl. 28.12.2020; opublik. 14.01.2021 – 1 c.

23. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2019660368 Rossiyskaya Federatsiya. Zamknutaya sreda predvaritel'nogo vypolneniya programm "TOR"/ V. A. Petrov, Ye. A. Maksimova, YU. N. Golubev, M. V. Ponomarev; zayavitel' Obshchestvo s ogranichennoy otvetstvennost'yu «Regional'nyy attestatsionnyy tsentr». – № 2019619100: zayavl. 24. 07. 2019: opubl. 05. 08. 2019 – 1 c.

24. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2015662413. Rossiyskaya Federatsiya. Otsenka effektivnosti sistemy zashchity informatsii / A. V. Pet'kiyev, Ye. A. Maksimova; pravoobladatel' FGAOU VO VolGU. – №2015619218, zayavl. 05. 10. 2015 g.; opublik. 24. 11. 2015. – 1 c.

25. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2012618761. Rossiyskaya Federatsiya. Sintez sistemy zashchity / Maksimova, V. A. Korneva; pravoobladatel' FGAOU VO VolGU. – № 2012616588; zayavl. 01. 08. 2012; opublik. 26. 09. 2021. – 1 c.

26. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 20216666613 Rossiyskaya Federatsiya. Otsenka infrastrukturnoy tselostnosti sub"yekta kriticheskoy informatsionnoy infrastruktury / Ye. A. Maksimova; zayavitel' Federal'noye gosudarstvennoye avtonomnoye obrazovatel'noye uchrezhdeniye vysshego obrazovaniya «Volgogradskiy gosudarstvennyy universitet». – № 2021665746: zayavl. 12. 10. 2021: opubl. 18. 10. 2021 – 1 c.

27. MentalModeler [Электронный ресурс]: sayt. – Rezhim dostupa: http://www.mentalmodeler.org/

28. SPPR «IGLA» [Elektronnyy resurs]: sayt. – Rezhim dostupa: http://iipo.tu-bryansk.ru/quill/download.html.

29. Analitika otrasli informatsionnoy bezopasnosti [Elektronnyy resurs]: sayt. – Rezhim dostupa: https://www.infowatch.ru/analytics/analitika.

МАКСИМОВА Елена Александровна, кандидат технических наук, доцент, доцент кафедры КБ-2 «Прикладные информационные технологии» института кибернетики и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет». Российская Федерация, 119454, ЦФО, г. Москва, Проспект Вернадского, д. 78. E-mail: maksimova@mirea.ru

MAKSIMOVA Elena Alexandrovna, Candidate of Technical Sciences, Associate Professor, Department of KB-2 "Applied Information Technologies" of the Institute of Cybernetics and Digital Technologies 1FGBOU VO "MIREA - Russian Technological University". Russian Federation, 119454, CFD, Moscow Moscow, Prospect Vernadsky, 78. E-mail: maksimova@mirea.ru.

БУЙНЕВИЧ Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России. Российская Федерация, 196105, СЗФО, г. Санкт-Петербург, Московский проспект, д. 149. E-mail: bmv1958@yandex.ru

BUINEVICH Mikhail Viktorovich, Doctor of Technical Sciences, Professor, Professor, Department of Applied Mathematics and Information Technology, St. Petersburg State Fire Service University EMERCOM of Russia. Russian Federation, 196105, NFD, St. Petersburg, Moskovsky Prospect, 149. E-mail: bmv1958@yandex.ru