Информационно-измерительные и управляющие системы

DOI 10.66032/2221-2574-2026-1-1-67-78 УДК 621.39

РАЗРАБОТКА АЛГОРИТМОВ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Лепешкин Олег Михайлович
доктор технических наук, доцент, профессор Высшей школы техносферной безопасности, Инженерно-строительный институт Санкт-Петербургского Политехнического университета[1] Петра Великого.

Остроумов Олег Александрович
кандидат технических наук, преподаватель кафедры, Военная орденов Жукова и Ленина краснознамённая академия[2] связи им. Маршала Советского союза С.М. Будённого.

Синюк Александр Демьянович
доктор технических наук, доцент, профессор кафедры общепрофессиональных дисциплин, Военная орденов Жукова и Ленина краснознамённая академия[2] связи им. Маршала Советского союза С.М. Будённого.

[1]*Адрес:* 194064, Российская Федерация, г. Санкт-Петербург, Политехническая улица д. 29.
[2]*Адрес:* 194064, Российская Федерация, г. Санкт-Петербург, Тихорецкий просп., д. 3.

E-mail для связи: lepechkin1@yandex.ru

Аннотация: нормативными документами в области обеспечения безопасности объектов критической инфраструктуры определена необходимость категорирования таких объектов. Данный процесс представляет собой ряд мероприятий, выполняемых комиссией, назначенной руководителем организации. Процедура определения категории в различных сферах деятельности организации является трудозатратной, при этом в любой момент времени значение объекта критической информационной инфраструктуры может меняться, что приведёт к необходимости изменения категории значимости. Данные условия определили необходимость автоматизации процесса категорирования для своевременного выявления изменений состояния объекта и снижения затрат на процесс категорирования. Целью исследования является разработка алгоритмов категорирования объектов критической информационной инфраструктуры для дальнейшего их использования при создании программного средства категорирования таких объектов. Результаты: разработаны алгоритмы определения категории значимости объектов критической информационной инфраструктуры в социальной, политической, экологической сферах, а также значимости для обеспечения обороны страны, безопасности государства и правопорядка. Автоматизация процесса категорирования объектов критической информационной инфраструктуры позволит уменьшить затраты на него, а также своевременно реагировать на необходимость её изменений. Практическая значимость: результаты исследования могут быть использованы при работе комиссий по категорированию объектов критической информационной инфраструктуры, а также для разработки программного продукта.

Ключевые слова: критическая информационная инфраструктура, категорирование, комиссия по категорированию, мероприятия категорирования объектов критической информационной инфраструктуры.

Введение

С первого января 2018 года вступил в силу ФЗ № 187 от 26 июня 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — закон). В соответствии с ним на субъекты критической информационной инфраструктуры (КИИ) осуществляют присвоение одной из категорий значимости объектам КИИ (ОКИИ). Сведения о присвоении или отсутствии такой необходимо-

сти субъекты КИИ предоставляют в федеральный орган исполнительной власти. Разделение объектов КИИ производится по критериям значимости. В законе определено пять критериев отнесения объектов к КИИ: социальная, политическая, экологическая, экономическая значимости и значимость для обеспечения обороны страны, безопасности государства и правопорядка. Кроме этого, каждый показатель делится на три категории. Категорирование критически важных объектов имеет целью определение перечня средств защиты для обеспечения устойчивого функционирования такого объекта [1–3].

После проведения процедуры категорирования, которую проводит назначаемая руководителем субъекта КИИ комиссия, определяется необходимый уровень защиты для ОКИИ. Работа комиссии требует определённых затрат. Комиссия в любой момент времени, в течении которого она работает, должна быть способна зафиксировать факт необходимости изменения категории значимости объекта, что не всегда возможно. Все это определило актуальность и цель исследования, направленных на автоматизацию процесса категорирования ОКИИ, разработку алгоритмов автоматизированного категорирования ОКИИ, позволяющих в том числе фиксировать в режиме реального времени необходимость изменения категории значимости ОКИИ.

На практике специалисты, занимающиеся категорированием объектов КИИ, тратят много времени на этот процесс, при этом его можно сократить примерно на 15–20 % и более за счёт автоматизации процесса и наличия исходных данных об объекте категорирования. При этом только процесс сбора и актуализации информации, документов о ОКИИ, который является крупным предприятием или сложной технической системой может занять до нескольких месяцев [4]. Это актуально в нынешнее время, когда на рынке труда существует нехватка специализированных кадров. Для увеличения оперативности процедуры категорирования ОКИИ предлагается использовать методы автоматизации процесса, оптимизации процессов, планирования и прогнозирования.

Для категорирования и оценки показателей критериев значимости возможно использовать программные продукты, алгоритм работы которых основан на выполнении Закона, Постановления Правительства РФ № 162 от 17 февраля 2018 года «Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых ОКИИ РФ» и Постановления Правительства РФ № 127 от 8 февраля 2018 года «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» (далее Постановление Правительства (ПП))

Примерами разработки средств автоматизации процесса категорирования объектов КИИ может быть автоматизированная система UDV ePlat4m, используемая для информационно-технической поддержки процесса категорирования. Предложенная система позволяет вести реестр объектов КИИ, угроз таким объектам, подготовку отчётной документации.

Ещё одним решением в области информационной безопасности ОКИИ является информационно-справочная система «Альфадок», в которой также есть возможность формирования отчётных документов при категорировании ОКИИ.

Средства SGRC, в частности, комплекс «Купол.Документы», позволяют осуществлять сбор и обработку информации о ОКИИ, подготовку соответствующей документации на этапах категорирования, а также производить расчёты категории значимости и формировать списки угроз и средств защиты от них. Комплекс является пилотным и проходит апробацию на 30 предприятиях в 8 регионах РФ.

Категорирование предназначено для выявления, на что влияет нарушение или прекращение функционирования объекта КИИ и какие меры противодействия этому необходимо использовать для предотвращения такого нарушения [5–7].

Категорирование сложных технических систем, как ОКИИ

Процедуру категорирования ОКИИ, исходя из закона и ПП, можно разделить на следующие этапы:

1. Создание по решению руководителя субъекта КИИ постоянно действующей комиссии и издание документа о её назначении, где определяются её полномочия и задачи.

Состав комиссии законодательно регламентирован и включает должностных лиц, указанных в статье 11 ПП и включение которых обязательно. Здесь же руководителю субъекта КИИ предоставляется право включения в состав комиссии специалистов по его усмотрению. При утрате объектом признаков объекта КИИ или прекращения ими деятельности в сферах, указанных в законе, комиссия по категорированию подлежит расформированию.

2. Сбор и обобщение исходных данных об объектах категорирования, принадлежащих субъекту КИИ.

Для категорирования, как правило, используются следующие исходные данные:

– основные сведения об ОКИИ (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими ОКИИ, наличие и характеристики доступа к сетям связи) [8, 9];

– основные сведения о управленческих, технологических, производственных, финансово-экономических и (или) иных процессах, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ, т.е. о критических процессах [10, 11];

– состав информации, обрабатываемой ОКИИ, сервисы по управлению, контролю или мониторингу, предоставляемые объектами КИИ [12];

– основное содержание декларации промышленной безопасности опасного производственного объекта, декларации безопасности гидротехнического сооружения и паспорт безопасности объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует ОКИИ;

– сведения о взаимодействии ОКИИ с другими ОКИИ и (или) о зависимости функционирования ОКИИ от других таких объектов [13];

– перечень угрозы безопасности информации в отношении ОКИИ, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на ОКИИ соответствующего типа [5, 8, 14].

3. Определение критических процессов в работе СТС.

Отследить появление новых критических процессов, а также процессов, их обеспечивающих, в режиме реального времени без автоматизации довольно проблематично для СТС в процессе их функционирования. Это создаёт предпосылки к несвоевременному выявлению необходимости категорирования объекта, необходимости изменения категории его значимости, а также необходимость автоматизации, как минимум, выявления таких изменений в работе СТС.

4. Определение перечня объектов, систем, процессов, обеспечивающих выполнение критических процессов в СТС и (или) осуществление управления ими, их мониторинг [15].

5. Формирование перечня объектов, субъекта КИИ, подлежащих категорированию.

6. Оценка масштабов последствия нарушения функционирования ОКИИ, не выполнения критических процессов при возникновении компьютерных инцидентов. Также должен проводится анализ угроз безопасности информации, которые могут привести к нарушению функционирования объекта КИИ и возможных действий нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации.

7. Проведение процедуры категорирования объектов СТС и присвоение каждому объекту категории значимости, принятие решения об отсутствии необходимости присвоения.

8. Разработка отчётных документов работы комиссии по определению категории значимости ОКИИ.

Результаты работы комиссии по категорированию оформляются актом, который подписывается всеми членами комиссии и утверждается руководителем субъекта КИИ. Результатами работы комиссии, в зависимости от перечня потенциальных угроз, может быть перечень сценариев действий системы при нарушении её функционирования при воздействии на неё [14].

9. Предоставление информации об ОКИИ в ФСТЭК.

Данная информация включает сведения об объекте и субъекте КИИ, о взаимодействии ОКИИ с сетями электросвязи, о программных и программно-аппаратных средствах на ОКИИ, о потенциальных нарушителях, угрозах безопасности, риски последствий нарушения функционирования ОКИИ при возникновении инцидентов, категорию значимости ОКИИ и организационные и технические меры, используемые для обеспечения безопасности ОКИИ.

10. Разработка руководителем субъекта КИИ документа, регламентирующего предоставление данных об инцидентах в ГосСОПКА (ФСБ РФ).

Рассмотрим более подробно процедуру присвоения категории значимости ОКИИ. При расчётах учитывается наиболее худший вариант последствий нарушения функционирования ОКИИ, как указано в ПП. Определение категории социальной значимости для объектов КИИ включает пять этапов, представленных на рис. 1. Для определения ущерба жизни и здоровью оценивается потенциальное количество людей, которые пострадают в случае нарушения функционирования объекта КИИ. При расчете потерь необходимо учитывать влияние нарушения функционирования объекта, людей, находящихся на объекте (смены, графики работы, численность находящихся на объекты в разное время суток и т.д.), а также влияние нарушения функционирования объекта на людей близлежащих населённых пунктов.

Для расчёта потерь и ущерба жизни и здоровью людей можно использовать методы и методики, а также математический аппарат предложенные, например, в работах [16–18].

При оценке влияния прекращения/нарушения функционирования объектов жизнеобеспечения населения производится анализ невыполнения/нарушения выполнения функций объекта КИИ, влияющих на удовлетворение потребностей жизнедеятельности населения, для чего определяется количество людей, зависящих от функционирования объекта КИИ, выявляют процессы обеспечения водо-, тепло-, газо-, электроснабжения, доставки продовольствия, обеспечения связи и управления и контроля этих процессов и т.д.

Для расчёта данного показателя используются статистические данные, характеризующие максимальное количество населения, которое является потребителем услуг, предоставляемых ОКИИ. Для расчета показателя транспортной доступности можно использовать следующее выражение

$$y_{\text{тр}} = (N_{\text{о}} - N_{\text{н}})k_{\text{ск}} + N_{\text{п}}k_{\text{сп}}, \qquad (1)$$

где $N_{\text{о}}$ — общее количество населения, проживающего на территории, обслуживаемым объектом транспортной инфраструктуры; $N_{\text{н}}$ — количество населения, проживающего на территории, обслуживаемым объектом транспортной инфраструктуры и не пользующаяся транспортом; $k_{\text{ск}}$ — сезонный коэффициент коренного населения, изменяющийся в пределах от 0 до 1, характеризующий временную убыль коренного населения, которое не пользуется инфраструктурой (уменьшение значения происходит в летний период, каникулы, праздники, когда население уезжает на отдых); $N_{\text{п}}$ — общее количество приезжающего на территорию населения на отдых; $k_{\text{сп}}$ — понижающий сезонный коэффициент приезжих, изменяется от 0 до 1, максимум в летний период, праздники.

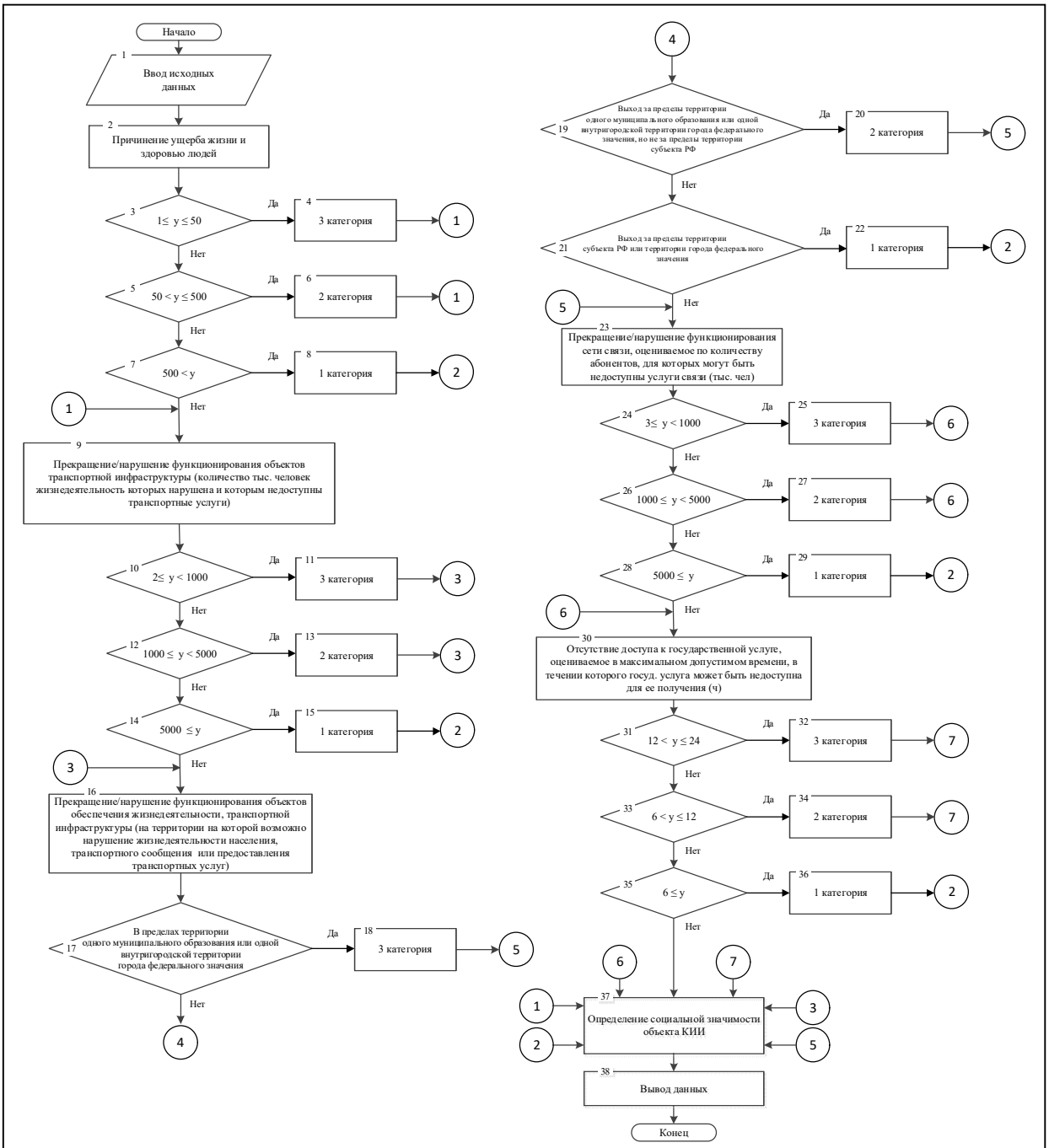

Рис. 1. Алгоритм определения социальной значимости ОКИИ

Для расчёта показателя доступности услуг связи можно использовать следующее выражение

$$y_{\text{ус}} = \max(N_{11} \le N_{12} \le \ldots \le N_{1i}) + \\ + \max(N_{21} \le N_{22} \le \ldots \le N_{2i}), \qquad (2)$$

где i — количество операторов связи; N_{1i} — количество человек местного населения, использующих i-го оператора по месяцам года; N_{2i} — количество приезжих, использующих i-го оператора по месяцам года.

Зависимость населения, проживающего на определённой территории, от функционирования транспортной инфраструктуры и её объектов позволяет проводить оценку влияния нарушения их функционирования.

Невозможность определённого количества абонентов системы и сетей связи получать услу-

гу связи, как и время отсутствия доступа у населения к получению государственных услуг, позволяют оценивать социальную значимость ОКИИ.

Оценка политической значимости объекта КИИ осуществляется в соответствии с алгоритмом, представленным на рис. 2, на основании оценки возможности государственного органа, администрации Президента РФ, Правительства РФ, Федерального собрания РФ, Совета Безопасности РФ, Верховного и Конституционного судов РФ, выполнять возложенные на них функции.

Оценка экономической значимости объекта КИИ осуществляется в соответствии с алгоритмом, представленным на рис. 3. Данная оценка проводится на основании статистических (прогнозируемых) данных за определённый период времени в количественном эквиваленте среднедневных совершенных операций или годового объёма доходов, а также в полном прекращении проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ. Данный критерий оказывает существенное влияние на экономику страны в целом, а также на процесс функционирования объектов КИИ, подверженных воздействию различных дестабилизирующих факторов, наибольшую опасность для которых представляют компьютерные атаки.

Для расчёта экономической значимости по блоку 2 рис. 3 может быть использовано выражение

$$y_{\text{э}} = \frac{F_{\text{пл}} - (F_{\text{п}} - F_{\text{у}})}{F_{\text{пл}}}, \qquad (3)$$

где $F_{\text{пл}}$ — планируемый доход, $F_{\text{пл}} = (F_i + F_{i-1} + F_{i-2} + F_{i-3} + F_{i-4})/5$; i — год предыдущий оценки; F_i — доход за i-й год; $F_{\text{п}}$ — фактически полученные доходы за текущий год; $F_{\text{у}}$ — фактический ущерб, нанесённый предприятию за текущий год.

Для расчёта экономической значимости по блоку 9 рис. 3 может быть использовано выражение

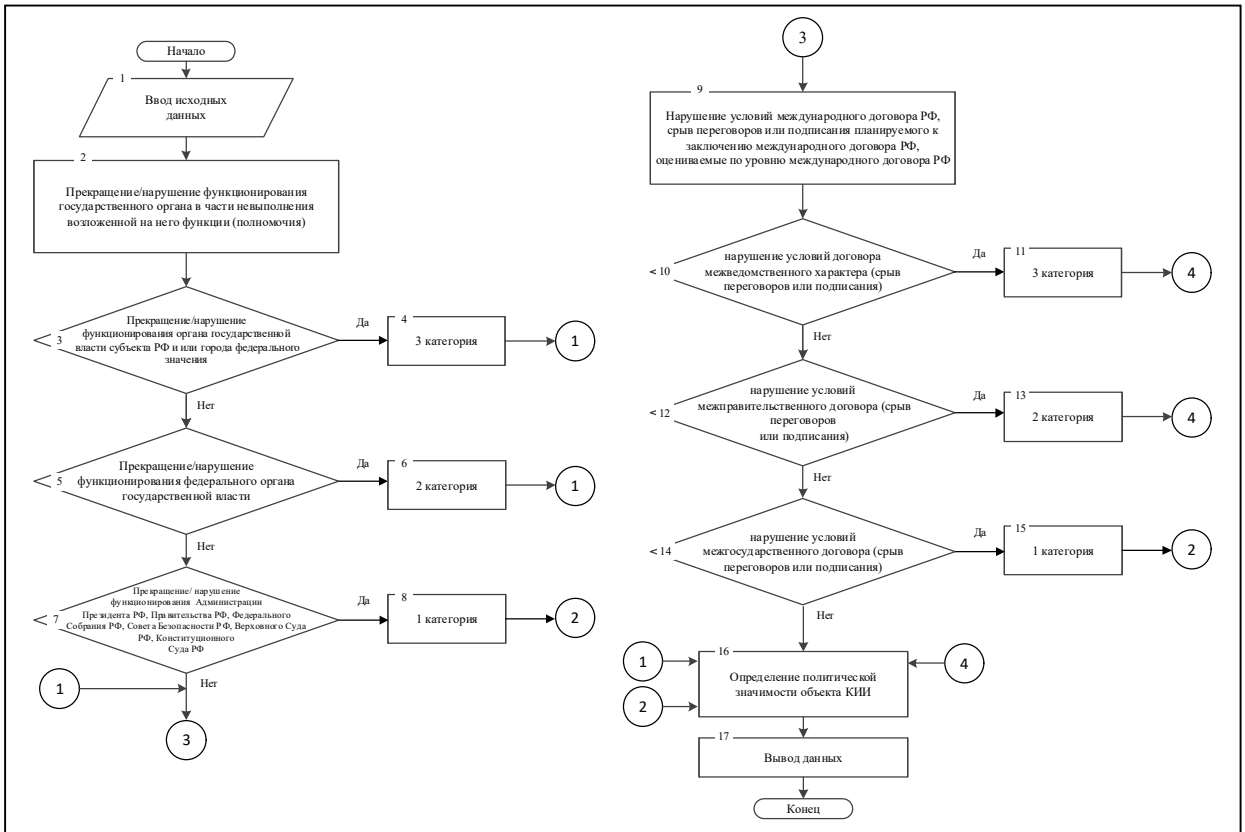

Рис. 2. Алгоритм определения политической значимости объекта КИИ

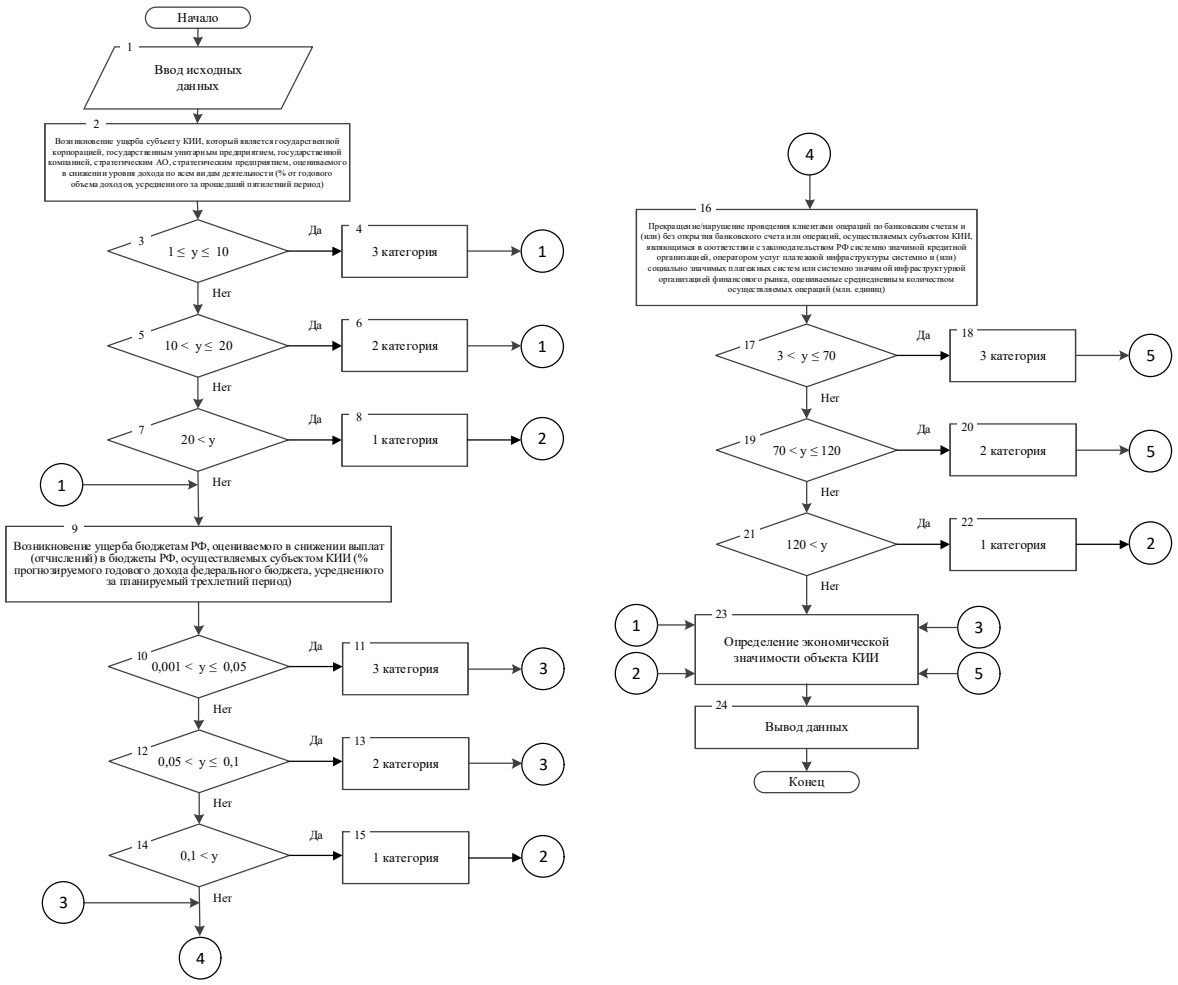

Рис. 3. Алгоритм определения экономической значимости объекта КИИ

$$y_э = \frac{F_{пл} - (F_п - F_у) * H}{F_{пл}}, \qquad (4)$$

где $F_{пл}$ — планируемые отчисления в бюджет РФ, $F_{пл} = (F_i + F_{i-1} + F_{i-2})/3$; i — год предыдущей оценки; F_i — доход за i-й год; $F_п$ — фактически полученные доходы за текущий год; $F_у$ — фактический ущерб, нанесённый предприятию за текущий год; H — налоговая ставка по которой осуществляется налогообложение объекта для поступления средств в бюджет РФ.

Хотелось бы заметить, что не поступление средств в бюджет субъекта РФ при нарушении функционирования объекта также является основанием для отнесения его к ОКИИ и создания соответствующей системы обеспечения безопасности его функционирования. Для оценки значимости объектов КИИ по блоку 16 рис. 3 используется статистика по выполнению среднедневных (за год) финансовых операций клиентами объекта КИИ.

Оценка экологической значимости объекта КИИ производится на основании алгоритма, представленного на рис. 4. Показателями экологической значимости объекта является потенциальное вредное воздействие, оказываемое на население (количество людей) и окружающую среду на определённой территории РФ.

Ущерб от аварий, в которых участвует ОКИИ, комиссией по категорированию может приниматься, как средство оценки экологического ущерба от нарушения функционирования ОКИИ. Могут использоваться сценарии и данные, указанные в паспортах безопасности и других документов, разработанных для ОКИИ, для которого проводится процедура категорирования.

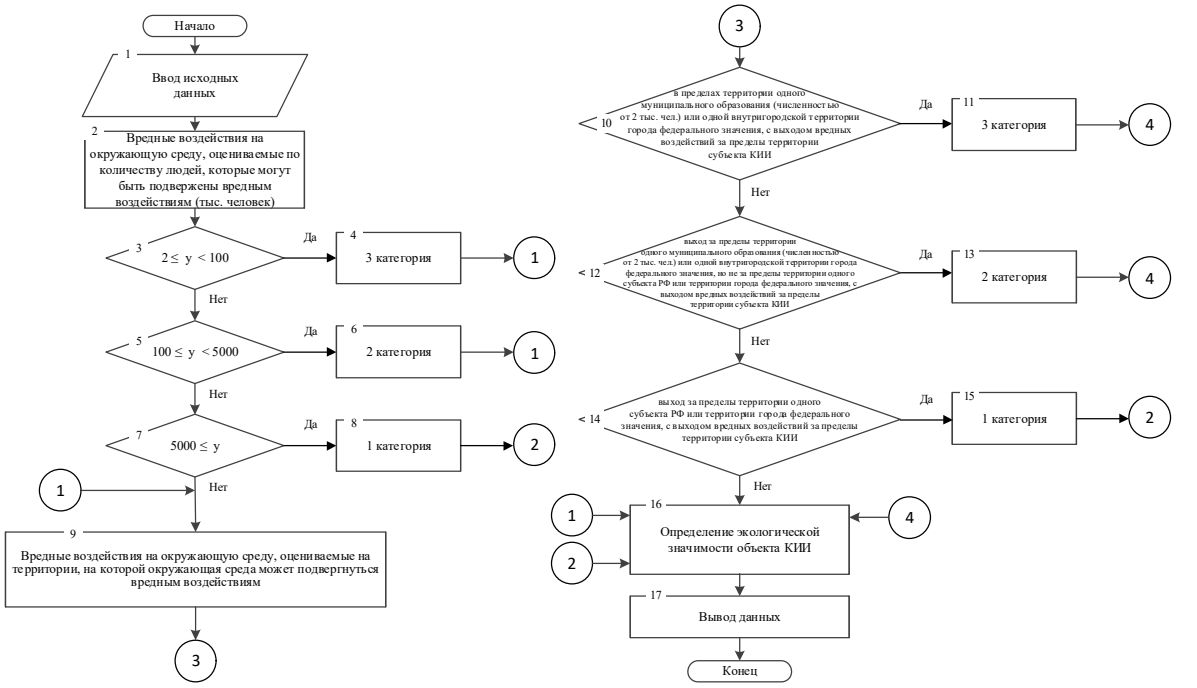

Рис. 4. Алгоритм определения экологической значимости ОКИИ

Для оценки экологической значимости ОКИИ (блок 2 рис. 4) может использоваться следующее выражение

$$y_э = (N_1 - N_2) \mid S \le S_{max}, \qquad (5)$$

где N_1 — количество людей, проживающих на территории РФ; N_2 — количество людей, проживающих вне зоны поражения при нарушении функционирования ОКИИ; S — зона поражения при нарушении функционирования ОКИИ; S_{max} — максимальная возможная зона поражения при нарушении функционирования ОКИИ.

Для оценки зоны поражения объекта КИИ могут использоваться методики, указанные в [19–21].

Определение значимости объекта для обеспечения обороны страны, безопасности государства и правопорядка осуществляется в соответствии с алгоритмом, представленным на рис. 5. Основными критериями оценки значимости объекта являются процентное снижение гособоронзаказа, нарушение функционирования пунктов управления ситуационных центров различных уровней, а также отсутствие доступа к услугам информационных систем в течение определённого времени.

Для оценки значимости ОКИИ для обороны РФ и правопорядка (блок 2 рис. 5) может использоваться следующее выражение

$$y_о = \frac{V_{пл} - V_{вып}}{V_{пл}}, \qquad (6)$$

где $V_{пл}$ — планируемый объем работ, услуг, выполняемых ОКИИ за период времени; $V_{вып}$ — фактически выполненный объём работ, услуг, выполняемых ОКИИ за период времени.

Для оценки значимости ОКИИ для обороны РФ и правопорядка (блок 9 рис. 5) может использоваться следующее выражение

$$y_о = \frac{t_ф - t_{вып}}{t_ф}, \qquad (7)$$

где $t_ф$ — фактическое время выполнения работ, услуг, выполняемых ОКИИ; $t_{вып}$ — планируемое время на выполнение заданного объёма работ, услуг, выполняемых ОКИИ.

Для оценки значимости ОКИИ для обороны РФ и правопорядка (блок 23, рис. 5) может использоваться следующее выражение

$$y_о = t_{пл} - t_{дост}, \qquad (8)$$

где $t_{дост}$ — время, в течение которого информационная система была доступна; $t_{вып}$ — время, в течение которого информационная система

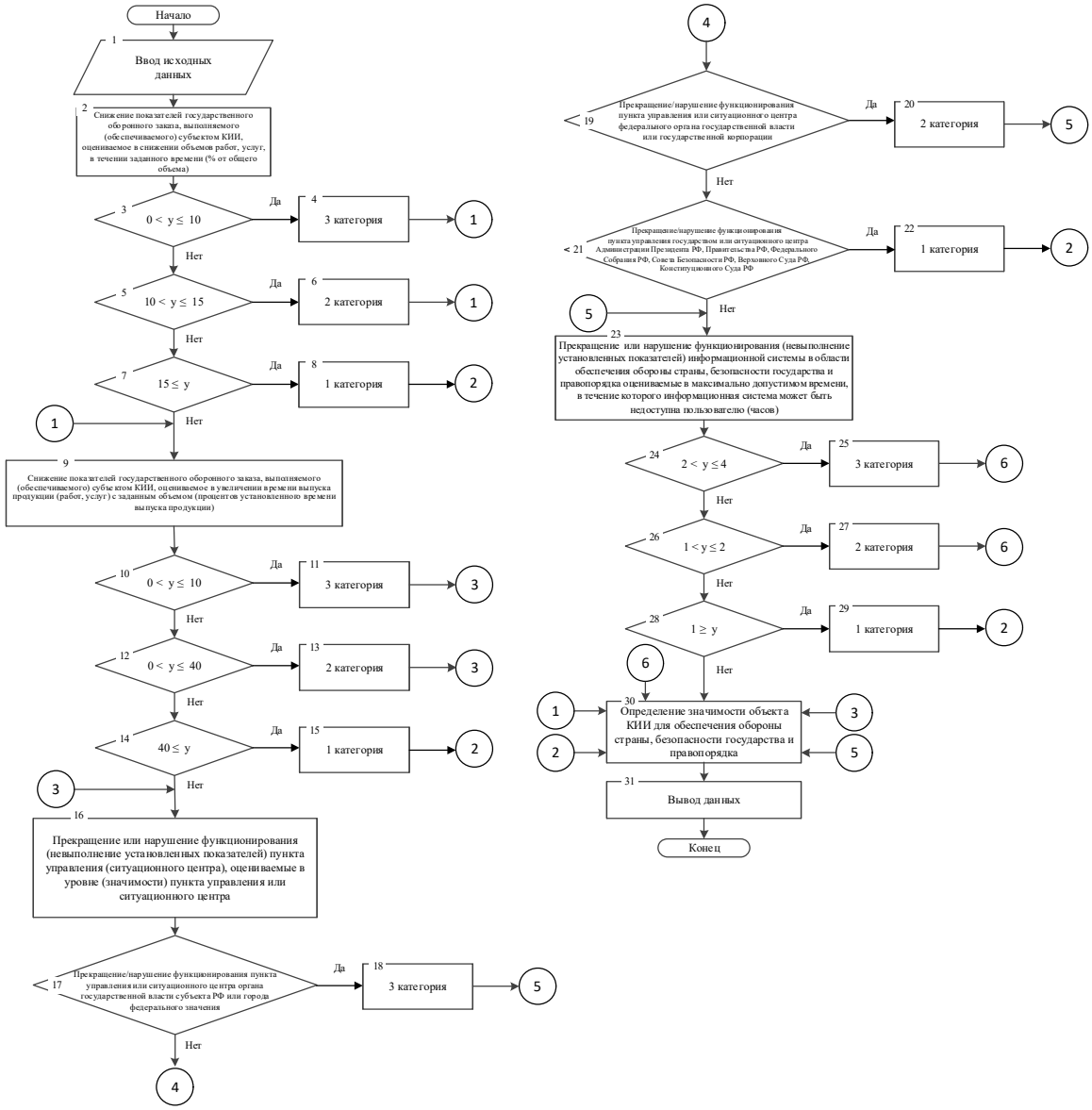

Рис. 5. Алгоритм определения значимости объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка

должна быть доступна. Значения $t_{дост}$ и $t_{вып}$ могут складываться из требуемых периодов времени.

Категория значимости системы и сетей связи, которые используются для обеспечения функционирования ОКИИ, должна быть не ниже категории значимости самого ОКИИ. Максимальная значимость по любому из критериев, определённых законом, определяет общую категорию значимости ОКИИ, которая присваивается на основе результатов работы комиссии по категорированию. Оценка категории значимости ОКИИ, для которого установлено более одного значения такого показателя категории значимости, осуществляется для каждого показателя и критерия, а общая значимость определяется по наивысшей категории.

Объекту, в отношении которого проводится процедура категорирования, категория значимости не присваивается, если ни один из показателей не применим, или по критериям показателей объект не соответствует ни одной из категорий.

Использование средств автоматизации процесса категорирования ОКИИ позволит сокра-

тить алгоритм действий руководителя субъекта КИИ и будет включать следующие этапы:

1. Установка программного обеспечения;

2. Внесение данных об объекте, в том числе с использованием открытых информационно-справочных систем, например, Росстата;

3. Определение перечня должностных лиц, которые будут включены в состав комиссии по категорированию. Внесение данных в программный продукт;

4. Генерация документов комиссии и отчётных документов категорирования ОКИИ;

5. Проверка сгенерированных документов членами комиссии и их подписание;

6. Отправка документов регуляторам в ФСТЭК и ФСБ.

Вывод

На основании ФЗ № 187 от 26 июля 2017 г. и Постановления Правительства РФ № 127 от 8 февраля 2018 г. разработаны алгоритмы, позволяющие осуществлять процедуру категорирования ОКИИ, которые будут использованы для разработки программного продукта для ЭВМ, что позволит автоматизировать процесс категорирования ОКИИ, отслеживать изменение состояния ОКИИ и осуществлять выявление фактов необходимости изменения категории. Направлениями дальнейших исследований является оценка рисков использования автоматизированных систем для категорирования ОКИИ.

Литература

1. *Иванов С.А.* Методика оценки информированности источника деструктивных воздействий о структуре корпоративной системы управления // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. №1–2 (163–164). С. 80–86.

2. *Остроумов О.А.* Модель контроля функционирования системы связи // Известия Тульского государственного университета. Технические науки. 2022. №3. С. 300–310.

3. *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. С. 37–48.

4. *Душа И.Ф.* Автоматизация процесса категорирования объектов критической информационной инфраструктуры в электросетевом комплексе // Энергия единой сети. 2024. №3–4 (74). С. 60–65.

5. *Kotenko I., Saenko I., Lauta O., Karpov M.* Methodology for management of the protection system of smart power supply networks in the context of cyberattacks // Energies. 2021. Vol. 14, №18. DOI: 10.3390/en14185963.

6. *Остроумов О.А.* Проблема обеспечения функциональной устойчивости систем критически важных объектов // Электросвязь. 2022. №1. С. 14–18.

7. *Тарасов А.А.* Проблема обеспечения гарантоспособности информационных систем и пути ее решения // Системы безопасности, связи и телекоммуникаций. 2000. №32. С. 78–80.

8. *Жиленков А.А., Черных С.Г.* Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. №2 (36). С. 58–66. DOI: 10.21681/2311-3456-2020-2-58-66.

9. *Аунг Чжо Мью, Анисимов А.А., Гагарина Л.Г., Портнов Е.М.* Методика повышения эффективности управления ресурсоемкими задачами в распределенных вычислительных системах // Инженерный вестник Дона. 2022. №2. URL: http://ivdon.ru/ru/magazine/archive/n2y2022/6294 (дата обращения: 11.07.2025).

10. *Vasiltsov V.S., Krylova N.P., Sushinskaya A.V.* et al. Information Analysis in Risk Management of BP (Using the Example of Metallurgical Enterprises) // Automatic Documentation and Mathematical Linguistics. 2024. Vol. 58, Iss. 3. Pp. 149–157. DOI: 10.3103/S0005105524700018.

11. *Ahmad I., Clark A., Ali M.* et al. Determining critical nodes in optimal cost attacks on networked infrastructures // Discover Internet of Things. 2024. Vol. 4, Iss. 1. Article 2. DOI: 10.1007/s43926-023-00054-1.

12. *Остроумов О.А.* Методика обеспечения функциональной устойчивости системы связи // Вопросы радиоэлектроники. Серия: Техника телевидения. 2022. Вып. 1. С. 3–12.

13. *Коцыняк М.А., Лаута О.С., Нечепуренко А.П.* Методика оценки устойчивости информационно–телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. №1–2 (127–128). С. 58–62.

14. *Zhang Y., Wang Z., Wang Y.* et al. A risk assessment model for similar attack scenarios in industrial control system // The Journal of Supercomputing. 2023. Vol. 79, Iss. 14. Pp. 15955–15979. DOI: 10.1007/s11227–023-05269-1.

15. *Menaceur A., Drid H., Rahouti M.* Fault Tolerance and Failure Recovery Techniques in Software-Defined Networking: A Comprehensive Approach //

Journal of Network and Systems Management. 2023. Vol. 31, Iss. 4. Article 83. DOI: 10.1007/s10922-023-09772-x.

16. *Косырев С.В., Матысик И.А., Свитнев И.В., Свитнев И.А., Хмелев В.Е.* Метод оперативной оценки возможных санитарных потерь при аварии на биологически опасном объекте // Технологии гражданской безопасности. 2014. №2 (40). С. 40–43.

17. *Грубеляс В.В., Савлучинский В.В., Саевич Т.Н.* Применение линейки оценки радиационной обстановки для прогнозирования величины структуры санитарных потерь // Военная медицина. 2018. №1. С. 2–6.

18. *Акимов В.А., Быков А.А., Востоков В.Ю., Ляховец Т.Л., Малышев В.П.* Методические рекомендации по определению количества пострадавших при чрезвычайных ситуациях техногенного характера // Проблемы анализа риска. 2007. Т. 4, №4. С. 347–367.

19. *Полуянов В.П.* Прогнозирование и оценка химической обстановки на объекте хозяйственной деятельности при аварии с выбросом опасного химического вещества // Вестник БГТУ имени В.Г. Шухова. 2008. №2. С. 83–85.

20. *Владимиров В.А., Исаев В.С.* Методика прогнозирования и оценки обстановки при выбросах в окружающую среду хлора и других аварийно химически опасных веществ // Стратегия гражданской защиты: проблемы и исследования. 2012. Т. 2, №1. С. 656–676.

21. *Акимов В.А., Иванова Е.О., Мишурный А.В.* Математическая модель для прогнозирования последствий разлива нефти и нефтепродуктов // Технологии гражданской безопасности. 2023. Т. 20, №1 (75). С. 68–70.

Поступила 12 июля 2025 г.

English

AUTOMATION OF THE PROCESS OF CATEGORIZING OBJECTS OF CRITICAL INFORMATION OF COMPLEX TECHNICAL SYSTEMS

Oleg Mikhailovich Lepeshkin — Grand Dr. in Engineering, Associate Professor, Professor of the Higher School of Technosphere Safety, Civil Engineering Institute of Peter the Great St. Petersburg Polytechnic University[1].

Oleg Aleksandrovich Ostroumov — PhD in Engineering, Lecturer of the Department, Military Orders of Zhukov and Lenin, Red Banner Academy[2] of Communications named after Marshal of the Soviet Union S.M. Budyonny.

Aleksandr Demyanovich Sinyuk — Grand Dr. in Engineering, Associate Professor, Professor of the Department of General Professional Disciplines, Military Orders of Zhukov and Lenin, Red Banner Academy[2] of Communications named after Marshal of the Soviet Union S.M. Budyonny.

[1]*Address*: 194064, Russian Federation, St. Petersburg, Politekhnicheskaya St., 29.
[2]*Address:* 194064, Russian Federation, St. Petersburg, Tikhoretsky Ave., 3.

E-mail: lepechkin1@yandex.ru

Abstract: Regulatory documents in the field of ensuring the security of critical infrastructure facilities define the need to categorize such facilities. This process is a series of activities carried out by a commission appointed by the head of the organization. The procedure for determining the category in various areas of the organization's activity is labor-intensive, while at any time the value of the critical information infrastructure object may change, which will lead to the need to change the significance category. These conditions determined the need to automate the categorization process for timely detection of changes in the state of the object and reduce the costs of the categorization process. The purpose of the study is developing algorithms for categorizing critical information infrastructure objects for their further use in creating a software tool for categorizing such objects. Results: algorithms have been developed for determining the significance category of critical information infrastructure objects in the social, political, environmental spheres, as well as significance for ensuring national defense, state security and law and order. Automation of the process of categorizing critical information infrastructure objects will reduce its costs, as well as promptly respond to the need for its changes. Practical significance: the results of the study can be used in the work of commissions for categorizing critical information infrastructure objects, as well as for developing a software product.

Keywords: critical information infrastructure, categorization, categorization commission, events for categorizing critical information infrastructure objects.

References

1. *Ivanov S.A.* Methodology for assessing the awareness of the source of destructive influences about the structure of the corporate management system. Issues of defense technic. Series 16: Technical means of countering terrorism. 2022. No. 1–2 (163–164). Pp. 80–86.
2. *Ostroumov O.A.* Model for monitoring the functioning of the communication system. Bulletin of Tula State University. Technical sciences. 2022. No. 3. Pp. 300–310.
3. *Klimov S.M., Polikarpov S.V., Ryzhov B.S., Tikhonov R.I., Shpyrnya I.V.* Methodology for ensuring the sustainability of the functioning of critical information infrastructure in the context of information impacts. Issues of cybersecurity. 2019. No. 6. Pp. 37–48.
4. *Dusha I.F.* Automation of the process of categorizing critical information infrastructure objects in the electric grid complex. Energy of a unified grid. 2024. No. 3–4(74). Pp. 60–65.
5. *Kotenko I., Saenko I., Lauta O., Karpov M.* Methodology for management of the protection system of smart power supply networks in the context of cyberattacks. Energies. 2021. Vol. 14. No. 18. DOI 10.3390/en14185963.
6. *Ostroumov O.A.* The problem of ensuring the functional stability of systems of critically important objects. Electrosvyaz. 2022. No. 1. Pp. 14–18.
7. *Tarasov A.A.* The problem of ensuring the reliability of information systems and ways to solve it. Systems of security, communication and telecommunications. 2000. No. 32. Pp. 78–80.
8. *Zhilenkov A.A., Chernykh S.G.* A system of accident-free management of critically important objects in the context of cyber attacks. Issues of cybersecurity. 2020. No. 2(36). Pp. 58–66. DOI: 10.21681/2311-3456-2020-2-58-66.
9. *Aung Kyaw Myu, Anisimov A.A., Gagarina L.G., Portnov E.M.* Methodology for improving the efficiency of managing resource-intensive tasks in distributed computing systems. Engineering Bulletin of the Don. 2022. No. 2. URL: ivdon.ru/ru/magazine/archive/n2y2022/6294 (Access date 11.07.2025).
10. *Vasiltsov V.S., Krylova N.P., Sushinskaya A.V.* Information analysis in risk management of BP (using the example of metallurgical enterprises). Autom. Doc. Math. Linguist. 2024. Vol. 58. Pp. 149–157. DOI: 10.3103/S0005105524700018.
11. Ahmad I., Clark *A., Ali M.* Determining critical nodes in optimal cost attacks on networked infrastructures. Discov Internet Things. 2024. Vol. 4. No. 2. DOI: 10.1007/s43926-023-00054-1.
12. *Ostroumov O.A.* Methodology for ensuring the functional stability of a communication system. Issues of Radio Electronics. Series: Television Engineering. 2022. Issue 1. Pp. 3–12.
13. *Kotsynyak M.A., Lauta O.S., Nechepurenko A.P.* Methodology for assessing the stability of an information and telecommunications network in conditions of information confrontation. Issues of defense technic. Series 16: Technical means of countering terrorism. 2019. No. 1–2 (127–128). Pp. 58–62.
14. *Zhang Y., Wang Z., Wang Y.* A risk assessment model for similar attack scenarios in industrial control system. J. Supercomput. 2023. Vol. 79. Pp. 15955–15979. DOI: 10.1007/s11227-023-05269-1.
15. *Menaceur A., Drid H., Rahouti M.* Fault tolerance and failure recovery techniques in software–defined networking: a comprehensive approach. J. Netw. Syst. Manage. 2023. Vol. 31. No. 83. DOI: 10.1007/s10922-023-09772-x.
16. *Kosyrev S.V., Matysik I.A., Svitnev I.V., Svitnev I.A., Khmelev V.E.* Method of operational assessment of possible sanitary losses in case of an accident at a biologically hazardous facility. Civil Safety Technologies. 2014. No. 2 (40). Pp. 40–43.
17. *Grubelyas V.V., Savluchinsky V.V., Saevich T.N.* Application of the radiation situation assessment ruler for forecasting the magnitude of the sanitary loss structure. Military Medicine. 2018. No. 1. Pp. 2–6.
18. *Akimov V.A., Bykov A.A., Vostokov V.Yu., Lyakhovets T.L., Malyshev V.P.* Methodical recommendations for determining the number of victims in man-made emergencies. Problems of risk analysis. 2007. No. 4. Pp. 347–367.
19. *Poluyanov V.P.* Forecasting and assessing the chemical situation at an economic facility during an accident with a release of a hazardous chemical substance. Bulletin of BSTU named after V.G. Shukhov. 2008. No. 2. Pp. 83–85.
20. *Vladimirov V.A., Isaev V.S.* Methodology for forecasting and assessing the situation during emissions of chlorine and other emergency chemically hazardous substances into the environment. Civil Defense Strategy: Problems and Research. 2012. Vol. 2. No. 1. Pp. 656–676.
21. *Akimov V.A., Ivanova E.O., Mishurny A.V.* Mathematical model for predicting the consequences of an oil and oil product spill. Civil Safety Technologies. 2023. No. 1(75). Pp. 68–70.