АНАЛИТИКА

УДК 004

КОНЦЕПЦИЯ, МЕТОДОЛОГИЯ И ТЕХНОЛОГИЯ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ НЕПРЕРЫВНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ, ИНТЕГРИРОВАННОЙ С ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ МЧС РОССИИ

Аннотация

Представлены концептуальные положения, методология и технология построения и функционирования непрерывной образовательной среды информационной безопасности и защиты информации, интегрированной с информационной инфраструктурой МЧС России, в интересах повышения уровня профессиональных компетенций должностных лиц и специалистов по защите информации.

Материалы предназначены для руководителей и специалистов-организаторов образовательной деятельности в области информационной безопасности и защиты информации в интересах государственных и корпоративных информационных инфраструктур.

Материалы разработаны по результатам внедрения прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России в 2024-2025 годах.

Ключевые слова: концепция, методология, технология, непрерывная образовательная среда, информационная безопасность, киберсреда.

Введение

Представленные концептуальные положения, методология и технология построения и функционирования непрерывной образовательной среды информационной безопасности и защиты информации, интегрированной с информационной инфраструктурой МЧС России в интересах повышения уровня профессиональных компетенций должностных лиц и специалистов по защите информации разработаны кафедрой прикладной математики и безопасных информационных технологий, а также специалистов центра информационных и коммуникационных технологий Санкт-Петербургского университета ГПС МЧС России, в составе авторского коллектива: Буйневич М.В., Грызунов В.В., Метельков А.Н., Матвеев А.В., Максимов А.В., Папырина Е.В., Рассказов М.С., Синещук М.Ю., Тукмачева М.А., Уткин О.В. – под руководством А.В. Шестакова.

Проведенный анализ отечественной и зарубежной практики создания и применения цифровых технологий непрерывной образовательной среды в интересах подготовки, переподготовки и повышения квалификации специалистов по защите информации показал, что:

- понятие «образовательная среда» в ключевых документах федерального уровня, регламентирующих образование, не определено (за исключением Федеральных государственных образовательных стандартов дошкольного образования). Образовательная среда, как понятие и сущность, является предметом (объектом) развития методологических подходов педагогической науки и практики, а в общем понимании – это совокупность условий, в которых происходит воспитание, обучение и развитие человека;
- расширенное понятие «информационная образовательная среда» введено при информатизации образования нормативными техническими документами в 2009 году (например, ГОСТ Р 53620) при внедрении информационно-телекоммуникационных технологий (далее –

ИКТ) в образование, которая означает – система инструментальных средств и ресурсов, обеспечивающих условия для реализации образовательной деятельности на основе ИКТ. В последующем для обеспечения освоения обучающимися образовательных программ в полном объеме независимо от их местонахождения нормативными правовыми актами определено понятие «электронной информационной образовательной среды» как совокупность электронных образовательных ресурсов, средств ИКТ и автоматизированных систем. При внедрении цифровых технологий понятие «образовательная среда» объективно трансформируется в «электронную информационную образовательную среду» и далее – в «цифровую образовательную среду» или с учетом возможностей виртуализации образовательных ресурсов и территориальной доступности – в цифровую образовательную киберсреду;

- образовательная среда, в общем понимании, развивается в направлении технологической интеграции различных уровней образования в «цифровую непрерывную образовательную среду» или «цифровую непрерывную образовательную киберсреду» (далее – НОК);
- в образовательной среде для обучения, развития навыков и тренировок в области информационной безопасности (далее – ИБ) находят применение специфические технические средства обучения или сервисы цифровой образовательной среды, таких как киберполигоны, универсальных требований НОК ИБ к которым не сформировано;
- сегмент рынка киберполигонов формировался на протяжении нескольких десятилетий и в настоящее время достаточно развит, особенно судя по зарубежным образцам;
- основная цель создания киберполигонов за рубежом заключается в обеспечении апробации современных технологий противодействия киберугрозам и обучении специалистов в области ИБ, которые проводят университеты, а для силовых структур – проведение на их базе специальных операций в киберсфере;
- отечественный рынок киберполигонов в последние несколько лет бурно развивается, что, в том числе, обусловлено конструктивными выводами на основе опыта эксплуатации зарубежных программных средств, их сопровождения и поддержки.

Актуальность затронутой проблематики обусловлена:

- факторами и условиями обеспечения ИБ информационной инфраструктуры РФ;
- требованиями руководства государства и Федеральных органов исполнительной власти (ФОИВ);

Основными противоречиями, применительно к обсуждаемой проблематике нарастающим итогом, относятся:

- потребности в современных навыках специалистов в области ИБ и существующий уровень подготовки, и возможности учебно-материальной базы;
- переход провайдеров существующих киберполигонов к платным сервисам обучения, групповых кибертренировок, киберучений для государственных организаций и возросшими потребностями должностных лиц, отвечающих за ИБ, в частности, в подразделениях территориальных органов МЧС России, в непрерывной профессиональной подготовке.

Опыт Санкт-Петербургского университета ГПС МЧС России в организации подготовки, переподготовки и повышения квалификации в области ИБ подтверждает острую необходимость внедрения в образовательный процесс новых практико-ориентированных технологий. Возросшие ведомственные потребности в «дипломированных» квалифицированных специалистах в области ИБ привели к увеличению количества сотрудников, направляемых на переподготовку. Однако такой экстенсивных процесс сопровождается ростом «неоднородности» контингента обучающихся, для которого традиционные формы обучения специалистов недостаточно эффективны, т.к. ориентированы на однородный уровень (в смысле уровня подготовленности к освоению новых знаний). По опыту переподготовки обучающихся их базовое образование сильно разнилось: ИКТ, радиотехника, связь – всего 41% обучающихся, все остальные имели базовое образование по другим специальностям. Опыт работы по

специальности ИБ в диапазоне: без опыта – 20%, незначительный опыт (до года) – 60%, более 5 лет – 20%. Ликвидировать дефицит компетенций обучающихся в ограниченные сроки без внедрения новационных мер очень проблематично, а по факту – невозможно.

Научная проработка проблем совершенствования системы подготовки ведомственных кадров в области ИБ осуществляется вузом при поддержке Департамента образовательной и научно-технической деятельности и Департамента информационных технологий и связи МЧС России.

Результаты многолетних исследований ученых вуза подтвердили целесообразность создания киберполигона как объекта нового класса сервис ориентированных организационно-технических систем, что подтверждается обширными публикациями: в части отдельных аспектов предметной области, а именно: анализа рисков [1], проактивного управления систем [2] и их развитием [3], учета зарубежного [4] и отечественного опыта [5], в том числе правовых механизмов [6, 7]; механизмов сбора данных [8], выявления инсайдеров информационных систем [9], индикаторов [10] и данных пользователей [11]; обеспечения доверия систем [12, 13] и данных [14, 15]; криптографических методов [16] и IT-, VR-технологий в области ИБ [17]; доступа к образовательному контенту [18, 19]; методических, дидактических [20] и оценочных средств образовательных процессов [21]; программной реализации образовательных систем [22], семантических методов учебно-методических [23] и информационных средств [24], компетентностных моделей [25], их уровня [26], оценки [27], адаптации [28], базовых функциональных модулей архитектур систем [29]; концептуального, инфологического [30] и онтологического моделирования [31], синтеза систем [32, 33] и выбора оборудования [34], оценки качества [35] и технико-экономической оценки решений [36].

Организационно ведомственный киберполигон имеет трехуровневую архитектуру:

- верхний уровень должны представлять органы управления образовательной деятельностью подведомственных образовательных организаций и органы управления ведомственной системы обеспечения информационной безопасности (далее – СОИБ), которая регламентирована федеральными и локальными нормативными актами.
- средний уровень – органы управления образовательных организаций и заинтересованные организации и подразделения ведомственных территориальных органов;
- нижний уровень является исполнительным, непосредственно реализующим сервисы для обучения, кибертренировок и киберучений.

Технологическую основу должны составлять информационные ресурсы и коммуникационная инфраструктура с применением средств и систем защиты информации различного функционального назначения и различных отечественных производителей.

Предварительный анализ результатов поисковых исследований показал несомненную актуальность создания НОК ИБ на основе интеграции ведомственных образовательных и инфраструктурных ресурсов на базе ведомственного киберполигона.

Результаты выполненных работ близкой проблематики за последние 5 лет, федеральных и национальных проектов показали отсутствие приемлемых решений для НОК ИБ и достаточно интенсивную практическую направленность проектов, реализуемых на базе зарубежных образовательных центров, университетов для решения ведомственных, региональных и национальных проблем в сфере кибербезопасности и киберзащиты информационных ресурсов и информационной инфраструктуры.

Основными проблемными вопросами настоящей публикации являются формирование концептуальных положений, методологии и технологии НОК ИБ и ее системы управления на основе киберполигона МЧС России.

1. Концепция непрерывной образовательной среды информационной безопасности, интегрированной с ведомственной информационной инфраструктурой

Актуальность концептуальной проработки исследования непрерывной образовательной среды информационной безопасности обусловлена преемственностью приоритетов в стратегии научно-технологического развития Российской Федерации (далее – Стратегия), указанных в основных правовых документах Российской Федерации 2016 и 2024 годов, в части противодействия различным угрозам и деструктивным воздействиям, в том числе киберугрозам, как сформулировано в перечислении д) пункта 20 Указа Президента Российской Федерации от 01.12.2016 № 642 [37], продолжено и расширено в перечисление д) пункта 21 Указа Президента Российской Федерации от 28.02.2024 №145 [38]. Концептуальные, а затем и методологические подходы к построению ведомственной НОК ИБ являются потенциалом практического применения научно-технических результатов НИР, таких как «Вариант» (2023), «Модель» (2023), «Киберсреда» (2024), с учетом приоритетов Стратегии, который раскрывается поэтапно, параллельно с развитием ИБ ведомства на основе ведомственных нормативных актов.

Поисковые исследования цифровых технологий НОК ИБ направлены на применение новых знаний в интересах обучения, подготовки, переподготовки и повышения квалификации ведомственных специалистов в области ИБ, следовательно, относятся к прикладным научным исследованиям, как определено статьей 2 Федерального Закона [39].

В настоящее время известен ряд результатов применения новых знаний в области цифровой трансформации образования, изложенных в следующих релевантных работах.

Проблемы, опыт внедрения и перспективы цифровой образовательной среды в Российской Федерации освещены в работе [40]. Авторами обсуждаются основные результаты эксперимента по ее внедрению в рамках одноименного федерального проекта национального проекта «Образование», реализованного в 2020-2021 году на базе общеобразовательных организаций субъектов и контента информационных ресурсов сети Интернет (в частности, государственной информационной системы «Моя школа»).

Частным вопросам цифровой образовательной среды посвящены исследования: применительно к вузу – методологии (на базе структурно-функциональной модели) и технологии педагогического проектирования переподготовки инженеров [41]; интеграции онлайн-обучения на основе открытых образовательных ресурсов и электронных курсов различных вузов [42]; модели смешанного обучения [43]; методическому инструментарию управления информационными потоками учреждения образования и библиотеки [89]; цифровых технологий [44]; выбора (отбора) образовательных ресурсов [45].

Анализ научных работ и публикаций по проблематике цифровой образовательной среды выявил несоответствие сущностной трактовки термина «цифровая образовательная среда» авторами, которые его широко используют для любых уровней образования, установленных федеральным законодательством, например, для вузов [46], и определений термина, которые приняты в нормативных документах Российской Федерации, а также документах программно-целевого развития Минпросвещения России и Минцифры России в отношении общего образования.

Применительно к использованию знаний, полученных на основе фундаментальных и поисковых исследований для реализации образовательных программ, подготовки научных кадров высшей квалификации, переподготовки и повышения квалификации, известна концепция цифровой научно-образовательной среды [47]. Ее концептуальная модель нормативно была закреплена в 2021 году и базируется на концептах цифровой инфраструктуры, которая оперирует такими онтологиями как <сети>, <системы>, <базы данных>, <базы знаний>, <цифровые ресурсы>, и концептах интеграции и взаимодействия и онтологиях, в частности, <сфер образования и науки>, <государственных информационных систем и институтов промышленной собственности>, <ресурсы интернет и научно-технических библиотек>. Также регламентирована концептуальная модель интероперабельности цифровой научно-образовательной среды, которая структурирует не только способность к информа-

ционному обмену, но и использование полученной информации на техническом, семантическом, организационном, нормативно-правовом уровнях и уровне гармонизации требований. Вопросы управления цифровой научно-образовательной среды сведены до уровня управления интеграцией активов, образовательными траекториями, доступностью ресурсов (сервисов), а обеспечения информационной безопасности – к выполнению регламентированных требований системы менеджмента информационной безопасности [62].

Частными вопросами прикладных научных исследований по проблематике построения и функционирования цифровой научно-образовательной среды являются: управление наукоемким ресурсным потенциалом организаций [48], некоторые аспекты формирования в вузе новой инновационной среды [49] и устойчивой конкурентоспособности исследовательских университетов [50], академическое предпринимательство [51], информационной безопасности формируемых гетерогенных информационных систем (научно-образовательных организаций, государственных и корпоративных систем, граждан) [52]. Вместе с тем, цельного методологического подхода по заявленной проблематике не просматривается.

Аналогично семантическим несоответствиям термина «цифровая образовательная среда» имеется неоднозначность в трактовке термина «непрерывная цифровая образовательная среда». Примем в качестве исходного положения, что непрерывная цифровая образовательная среда является новой формой организации системы непрерывного образования. Соответственно необходимо выявить современное международное и национальное понимание «непрерывного образования» и ее среды.

Генеральной Ассамблеей ООН в 2000 году в составе важнейших принятых решений были такие инициативы, как Концепция и Программа «Цели развития тысячелетия» (ЦРТ, *по англ.* Millennium Development Goals), которые установили до 2015 года 8 целей по актуальным глобальным проблемам (нищеты, начального образования (создание возможностей получения начального школьного образования в полном объеме), детской смертности, заболеваний, всемирного партнерства. Отчет о достигнутых результатах ЦРТ [53] был рассмотрен ООН в 2015 году, а его на Генеральной Ассамблее одобрили итоговый документ «Преобразование мира: Повестка дня в области устойчивого развития на период до 20230 года», который широко известен как «Цели в области устойчивого развития» (ЦУР, *по англ.* Sustainable Development Goals), так как содержал 17 целей (ликвидация нищеты и голода, качественное образование и другие) и 169 задач; все это под текущем управлением Департамента по экономическим и социальным вопросам ООН (*по англ.* Department of Economic and Social AffairsSustainable Development) для мониторинга выполнения Набора глобальных показателей странами-членами ООН и ежегодного рассмотрения итогов. Цель 4 «Качество образования» определена как «Обеспечение всеохватного и справедливого качественного образования и поощрение возможности обучения на протяжении всей жизни для всех», декомпозирована на 10 задач, в 4-й из которых сформулировано:

во-первых, обеспечить доступ к недорогому и качественному профессионально-техническому и высшему образованию: уровень участия в видах обучения, профессиональной подготовки (4.3.1), и в профессионально-техническом образовании (4.3.3); коэффициент охвата высшим образованием (4.3.2);

во-вторых, увеличить число молодых и взрослых с востребованными профессионально-техническими навыками: доля обладающих навыками в области ИКТ (4.4.2), достигших минимального уровня цифровой грамотности (4.4.2); уровень образования по возрастным группам (4.43).

Европейская комиссия в 2000 году приняла «Меморандум образования длинною в жизнь» (*по англ.* A Memorandum on Lifelong Learning), в отечественных источниках именуемый как «Меморандум непрерывного образования» [54], который провозглашает всестороннюю учебную деятельность на постоянной основе для улучшения знаний, навыков и профессиональной компетенции. Принятие решения, как объясняет неправительственная организация Европейская ассоциация образования взрослых (*по англ.* The European Association for the Education of Adults, *аббр.* EAEA), базировалось на понимании, что развитие образовательной среды

помогает в трудоустройстве и работе, так как обучающиеся, как кадры компаний, становятся более креативными, стрессоустойчивыми и продуктивными, что, в свою очередь, приводит к конкурентоспособности компаний[1]. Дальнейшее развитие основных положений «Меморандума непрерывного образования» нашло в Манифестах EAEA последующего периода:

- в «Манифесте по образованию взрослых в XXI веке» (EAEA, 2016) указывается, что обучение на рабочем месте является одним из основных факторов, мотивирующим работников принимать участие в непрерывном обучении. В нем указывается важность идеи повышения уровня знаний и переквалификации, а также, что любое обучение положительно сказывается на занятости. Отмечается, что в сфере дистанционного обучения, несмотря на новые возможности технологий, снижется значимость социального взаимодействия, важного для многих обучающихся;
- в «Манифесте об обучении взрослых в 21 веке: сила и радость обучения» (Manifesto for Adult Learning in the 21st Century: The Power and Joy of Learning, 2019)[2], одним из принципов является наращивание потенциала и инновации в образовании взрослых, необходимость для организаций адаптации и предвидения изменений потребностей в обучении и преподавании;
- в «Новом Манифесте об обучении взрослых в 21 веке: сила и радость обучения» (The new Manifesto for Adult Learning in the 21st Century: The Power and Joy of Learning, 2024) указаны базовые, цифровые и языковые навыки, ключевые компетенции (финансовой, медицинской и медиаграмотности).

В нашей стране официально понятие «непрерывное образование» введено на государственном уровне в период «Перестройки» в 1986 году применительно к экономическому образованию специалистов с высшим образованием с целью улучшения качества их подготовки для народном хозяйства [55], расширено в дальнейшем правовыми актами РФ, в частности:

- в 1992 году непрерывное повышение квалификации в пределах каждого уровня профессионального образования при определении основной задачи дополнительного образования в связи с постоянным совершенствованием ФГОС [56];
- в 1996 году как непрерывность и преемственность процесса образования в принципах государственной политики в области в области высшего и послевузовского профессионального образования [57];
- в 1996 году при определении задач государственной политики на рынке труда для поддержки качества рабочей силы через развитие системы непрерывного образования [58].

В дальнейшем понятие «система непрерывного образования» и ее состав уточнялись.

Перечень регламентированных Правительством Российской Федерации в 2013 году индикаторов развития системы непрерывного образования с целью мониторинга системы образования [59] содержал:

- показатели обучения (в системе высшего образования; дополнительного профессионального образования и на рабочем месте);
- показатели участи в мероприятиях (тренинги, экскурсии и частные занятия);
- частные показатели самообразования.

Вводились изменения к программам непрерывного образования при реализации национальных проектов, например, в 2020 году – правила предоставления грантов в образовательных организациях высшего образования, реализующих дополнительные образовательные программы и программы профессионального обучения [60].

На организационно-техническое построение и эффективность ведомственной образовательной среды информационной безопасности существенное влияние оказывают:

- обострившиеся противоречия ***между фактическим уровнем***, механизмами обеспечения профессиональных компетенций, знаний, умений и навыков, сил (средств) СОИБ ***и возрастающей сложностью новых задач***, требующих оперативного решения в условиях неопределенности;

[1] https://eaea.org/why-adult-education-2/empl oyment-and-work/

[2] https://eaea.org/wp-content/uploads/2019/04/eaea_manifesto_final_web_version_290319.pdf

- неявные противоречия ***между полномасштабно проводимой цифровой трансформацией*** процессов образовательной среды, стремительным ростом многообразия показателей в принятой системе менеджмента качества образования, ***и динамичными условиями адаптации*** профессиональных, федеральных государственных образовательных стандартов, интегрированного применения различных систем менеджмента рисков, в том числе ИБ, в условиях «незрелости» цифрового права, комплексирования ведомственных показателей развития секторов экономики, установленных в национальных проектах;
- нарастающие противоречия ***между традиционными способами*** организации инфраструктуры образовательной среды, которые регламентированы в соответствии с ведомственными возможностями и полномочиями, как ФОИВ, на организационно-штатное обеспечение организационной и технической структуры образования в области ИБ и на выделенные финансовые ресурсы, в рамках плановых объемов государственных бюджетных средств, ***и новыми угрозами*** информационной безопасности, ростом их разнообразия, интенсивности и вариативностью на ведомственные информационные, коммуникационные ресурсы, ограниченные силы и средства ведомственной СОИБ.

В ведомственных программах цифровой трансформации введен контрольный показатель, характеризующий долю ведомственных должностных лиц (специалистов), не только участвующих в цифровой трансформации, но и прошедших обучение в области информационной безопасности. В программе МЧС России [61] плановые значения на период 2022-2024 годов составил 7% и 5% соответственно.

Научная новизна проблематики построения и функционирования НОК ИБ применительно к особенностям организации в подведомственных вузах обучения, подготовки, переподготовки и повышения квалификации должностных лиц, выполняющих профессиональную деятельность в области ИБ, а также потребностей профессиональных компетенций ведомственных территориальных подразделений, заключается в применении методологии структурно-параметрического синтеза, методов адаптивного управления и формализации условий существования организационно-технических систем нового класса при поэтапном развития их структурно-функциональных компонент с учетом передовых практик современных цифровых образовательных сред, образовательных, информационных технологий и технологий ИБ, а также рекомендаций регуляторов в области ИБ.

Практическая значимость НОК ИБ, на основе интегрированной ведомственных образовательных и инфраструктурных ресурсов обусловлена ограниченными существующими возможностями сил и средств ведомственной СОИБ реагировать на современные и прогнозируемые вызовы в области ИБ.

Целостная методологическая база развития технической политики ведомства в области ИБ посредством реализации работ по созданию НОК ИБ на основе интегрированных ведомственных образовательных и инфраструктурных ресурсов пока не сформирована.

Для решения таких масштабных наукоемких, но одновременно и практически ориентированных задач требуется высококвалифицированный коллектив, сгруппированный по направлениям:

- концептуальной и методологической проработки проблемных вопросов и определения системотехнических решений по построению и функционированию ведомственной НОК ИБ, в том числе системы управления и ИБ, как ядра киберсреды ведомственных образовательных и информационных ресурсов;
- формирования экспериментального функционального фрагмента интеграции образовательных и информационных ресурсов вуза и компонент ведомственной информационной инфраструктуры и ведомственной СОИБ;
- организации и проведения мероприятий (работ) по валидации системотехнических решений с учетом существующего научного задела и решений по ИКТ в образовании и технологиям ИБ в рамках рекомендаций регуляторов в области образования и ИБ.

Концепция построения непрерывной образовательной среды информационной безопасности, интегрированной с ведомственной информационной инфраструктурой

Ведомственная НОК ИБ – это совокупность образовательных ресурсов ведомственной системы непрерывного образования, взаимоувязанных управлением и нормативно-правовой, организационной, методической и информационной базой, предназначенных для решения ведомственных задач должностными лицами, выполняющими профессиональную деятельность в области информационной безопасности.

Под *образовательными ресурсами* понимается соответствующая инфраструктура образовательной организации, организационно и функционально выделенная под задачи НОК ИБ, цифровые активы (ресурсы и знания) в области ИБ и средства взаимодействия, в том числе с внешними активами, а также совокупность цифровых технологий.

Внешними активами могут выступать информационные ресурсы государственной информационной системы «Современная цифровая образовательная среда», электронные образовательные ресурсы, перечень которых утвержден Минобрнауки России, и другие.

Ведомственная НОК ИБ создается *для разрешения сложившихся противоречий* между:

- *требуемыми навыками* отражения компьютерных атак, компетенциями и знаниями в сфере компьютерных инцидентов *и технологическими возможностями* традиционной ведомственной организации профессиональной подготовки и повышения квалификации должностных лиц, выполняющих профессиональную деятельность в области ИБ;
- потребностями в применении разнообразных цифровых образовательных киберсред ведомственной СОИБ и ограниченными ресурсными возможностями ведомственных образовательных организаций;
- *высокой динамикой* ведомственной СОИБ *и продолжительным периодом плановой трансформации* ведомственных образовательных инфраструктур, совпадающим по темпам с трансформацией управления ее компонент в сфере ИБ.

Ведомственная НОК ИБ *предназначена для*:

- предметно-ориентированного непрерывного обучения в области кибербезопасности в интересах территориальных органов и подведомственных организаций с применением цифровых технологий, в том числе искусственного интеллекта, больших данных и технологий ИБ;
- информационной поддержки должных лиц органов (пунктов) управления ведомственной СОИБ;
- организации прикладных исследований (испытаний, проверок) технологий и средств кибербезопасности на основе ведомственной образовательной и информационной инфраструктуры.

Цель построения и функционирования ведомственной НОК ИБ заключается в повышении эффективности ведомственной СОИБ путем непрерывного повышения уровня компетенций должностных лиц, выполняющих деятельность в области ИБ, на основе интеграции образовательной и информационной инфраструктуры ведомства.

Основополагающие принципы построения и функционирования ведомственной НОК ИБ состоят в следующем:

Во-первых, ведомственная НОК ИБ реализует взаимоувязанный *единый организационно-технический и методический принцип* по формированию профессиональных знаний, умений, навыков и компетенций в области ИБ в соответствии с ФГОС, профессиональными стандартами, основными профессиональными образовательными программами в подведомственной системе среднего общего образования, в том числе кадетских классах и кадетских корпусах, высшего образования на всех уровнях профессионального образования, включая подготовку научных кадров высшей квалификации, дополнительного профессионального образования, подготовки на рабочих местах и самообразования должностных лиц, выполняющих профессиональную деятельность в области ИБ.

Во-вторых, ведомственная НОК ИБ реализует *принцип единства планирования, централизованной координации и контроля* реализации *комплекса* мер с учетом ведомственных

программных мероприятий в области образования, цифровой трансформации, цифрового развития и информационной безопасности.

В-третьих, ведомственная НОК ИБ создается и функционирует на *принципах единства научно-технической политики развития* (доразвертывания и дооснащения) и поддержания эксплуатационных характеристик сервисов образовательного трека, испытательного трека и трека кибертренировок (киберучений).

В-четвертых, ведомственная НОК ИБ строится и функционирует *на принципах цифровой научно-образовательной прикладной среды информационной безопасности* на основе ведомственной организационно-технической системы нового класса «киберполигон».

Ведомственный киберполигон содержит собственную информационную инфраструктуру на основе ИКТ, технологий ИБ в подсистемах поддержки принятия решений ведомственной СОИБ и ее подсистемах в образовательных организациях.

Ведомственный киберполигон представляет собой единую централизованную организационно-техническую систему в составе территориально-распределенных сегментов сил и средств, с сегментом управления на базе образовательного учреждения, уполномоченного по вопросам создания, развития и функционирования ведомственного киберполигона и его интегрированного применения в иерархической структуре СОИБ.

Средства ведомственного киберполигона помимо различных по именованию технических, программных, лингвистических, правовых, организационных средств, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений для обеспечения функционирования и применения образовательной инфраструктуры по целевому назначению, могут содержать различные по функциональности и техническим возможностям программные, программно-аппаратные, аппаратно-программные изделия, которые обозначены производителем как «киберполигон».

В-пятых, ведомственная НОК ИБ строится и функционирует *на основе принципов*:

- территориальной распределенности сил и средств образовательной среды и ведомственной СОИБ;
- интегрированности учебно-образовательной среды ИБ;
- рационального сочетания штатных и выделенных ресурсов сил (средств) при организации и предоставлении сервисов, с учетом ведомственных оперативных задач;
- разделения полномочий и ответственности между субъектами ведомственной НОК ИБ на основе правовых документов и регламентов ведомства.

Ведомственная НОК ИБ должна *организовать, формировать и предоставлять пользователям основные сервисы,* которые по функциям организации, формирования и предоставления пользователям имеют определенное технологическое перекрытие:

а) образовательного трека:

- профориентированного образования по направлению ИБ с применением компьютерно-моделирующей среды прототипов и цифровых двойников реальных фрагментов ведомственной информационной инфраструктуры;
- формирования, апробации и внедрения новых дидактических методов с применением территориально-распределенных средств киберполигона и виртуальных сред;
- формирования и регламентированного функционирования проактивной киберсреды информационной поддержки в ведомственной системе управления ИБ по проблемам текущей деятельности профильных подразделений и организаций, программно-целевого развития единого информационного пространства ведомственной проактивной киберсреды;
- сбора, обработки и предоставления сведений подразделениям о выявлении в треке киберполигона новых инцидентов по результатам мониторинга инцидентов в области ИТ и ИБ, реагирования на инциденты ИБ;
- выработки научно-обоснованных предложений для лиц, ответственных за реализацию политики ИБ, взаимосвязанных и согласованных мер киберзащиты организационного и технического характера;

• поддержки в актуальном состоянии информации об информационных ресурсах и информационной инфраструктуры ведомственных территориально-распределенных фрагментах;

б) испытательного трека:

• исследования проблемных аспектов кибербезопасности ведомственной информационной инфраструктуры;

• формирования документов методического и организационного обеспечения информационной безопасности ведомственной информационной инфраструктуры;

• технической поддержки компонент ведомственной СОИБ;

в) кибертренировок (киберучений):

• формирования групповых компетенций должностных лиц, выполняющих профессиональную деятельность в ведомственной СОИБ;

г) управления и безопасности:

• планирования и организации управления и безопасности ресурсов;

• коммуникационные сервисы управления;

• управления коммуникационной инфраструктурой;

• управления безопасностью;

• поддержки решений управления;

• логистической поддержки.

Сводный перечень сервисов треков ведомственной НОК ИБ представлен в таблице 1.1.

Таблица 1.1 – Сводный перечень сервисов треков

Трек кибертренировок (киберучений)	Трек образовательный	Трек испытательный	Трек управления и безопасности
1	2	3	4
1. Сервисы профориентированного образования по направлению ИБ с применением компьютерно-моделирующей среды прототипов и цифровых двойников реальных фрагментов информационной инфраструктуры.		1. Сервисы исследования проблемных аспектов кибербезопасности ведомственной информационной инфраструктуры.	1 Сервисы планирования и организации управления и безопасности ресурсов
2 Сервисы формирования групповых компетенций ДЛ, выполняющих профессиональную деятельность в ведомственной СОИБ.	2. Сервисы формирования, апробации и внедрения новых дидактических	2 Сервисы формирования документов методического и организационного обеспечения ИБ ведомственной информационной инфраструктуры.	2 Коммуникационные сервисы управления
3. Сервисы формирования и регламентированного функционирования киберсреды информационной поддержки ведомственной СОИБ в текущей деятельности и по программам развития.		3. Сервисы технической поддержки компонент ведомственной СОИБ.	3 Сервисы управления коммуникацион-ной инфраструктурой
4. Сервисы сбора, обработки и предоставления сведений о новых инцидентах.			4 Сервисы управления безопасностью
5. Сервисы выработки предложений по мерам киберзащиты.			5 Сервисы поддержки решений управления
	6. Сервисы поддержки в актуальном состоянии информации об информационной инфраструктуре.		6 Сервисы логистической поддержки

Ведомственная НОК ИБ организационно имеет трехуровневую структуру.

Результаты анализа типовых вариантов архитектур организации повышения уровня осведомленности персонала в области ИБ показывают, что применение сервисов внешнего или выделенного компонента (рисунок 1.2 а, б) не отличаются функциями и задачами управления в корпоративных организационных системах, являются достаточно затратными при дина-

мичном изменении задач ведомственной СОИБ и потребностей ДЛ в поддержке принятия решений в области ИБ.

Поэтому наиболее предпочтительной является архитектура управления в корпоративной организационной системе с интегрированным компонентом (рисунок 1.1 в) – киберполигоном. Первый уровень архитектуры представлен подразделениями управления СОИБ, второй – управления ИИ киберполигона, третий – управления эксплуатацией и обеспечения киберполигона.

В организационной структуре НОК ИБ первый уровень представлен ведомственными подразделениями управления ведомственной СОИБ, образовательной и научно-технической деятельностью.

Второй уровень представлен организационно-технической системой образовательной организации, которая содержит подразделения организации образовательной деятельности и обеспечивающих подразделений в сфере информационной инфраструктуры и ИБ, в том числе сегмент управления организационно-технической системой (ведомственной НОК ИБ).

Рисунок 1.1 – Место и роль киберполигонов в организационной архитектуре ведомственной СОИБ

Третий уровень представлен подразделениями организационно-технической системы образовательной организации, которые обеспечивают проведение занятий, управление и эксплуатацию информационной инфраструктуры ИБ.

Функциональная структура ведомственной НОК ИБ содержит функциональные подсистемы доступа, инфраструктурных, моделирующих сред и виртуализации, технологического ядра, а также управления и безопасности.

Основными функциями подсистемы управления и безопасности НОК ИБ на базе образовательного учреждения, уполномоченного по вопросам создания, развития и функционирования ведомственного киберполигона, являются:

- организация и управление предоставления пользователям сервисов различных треков с требуемым качеством и безопасности;
- мониторинг и визуализация организации и функционирования сервисов различных треков в соответствии с предназначением и задачами;
- управление в соответствии с запросами пользователей конфигурацией объектовой и пользовательской среды, включая средства защиты информации, сервисов треков киберполигона, мониторинг их состояния.

Функциональная подсистема доступа обеспечивает авторизованный доступ и доверенное подключение пользователей к сервисам треков НОК ИБ, предоставляемых по запросам.

Функциональная подсистема управления обучением обеспечивает формирование, предоставление и поддержание функционирования сервисов образовательного трека НОК ИБ, предоставляемых по запросам пользователей.

Функциональная подсистема киберучений обеспечивает формирование, предоставление и поддержание функционирования сервисов трека кибертренировок (киберучений) НОК ИБ, предоставляемых по запросам пользователей.

Функциональная технологическая подсистема обеспечивает кроссплатформенность взаимодействия функциональных подсистем для формирования, предоставления и поддержания функционирования сервисов НОК ИБ, предоставляемых по запросам пользователей.

Функциональная подсистема моделирующих сред обеспечивает создание и подключение моделирующих компонент в соответствии с сервисами треков НОК ИБ, предоставляемых по запросам пользователей.

Функциональная подсистема инфраструктурных сред и информационной безопасности обеспечивает создание фрагментов учебной (образовательной) инфраструктуры и информационной безопасности, по соответствующим запросам сервисов треков НОК ИБ.

Функциональная подсистема виртуализации обеспечивает создание изолированной программной среды, преобразование формата (параметров) запросов к ресурсам (функциям, сервисам), организацию процессов обработки информации, независимых от программных и аппаратных платформ информационной инфраструктуры образовательной организации.

Ведомственная НОК ИБ, как и любая организационно-техническая система, включает в свой состав различные виды обеспечения функциональных подсистем.

Организационное и нормативно-правовое обеспечение содержит:

а) отечественные нормативные правовые акты в сфере ИБ, темпы развития которой достаточно высокие (пример статистических данных представлен на рисунках 1.2 и 1.3, в таблице 1.2) [63];

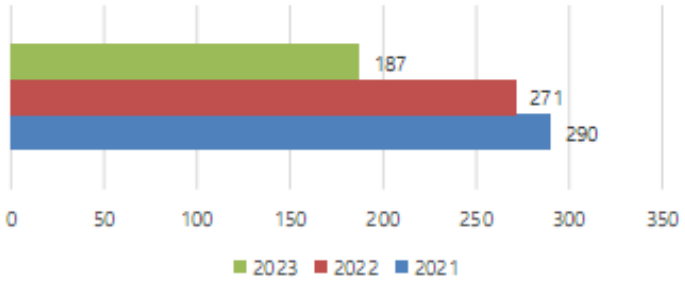

Рисунок 1.2 – Количество принятых документов и их проектов за 2021-2023 год (Источник: [27])

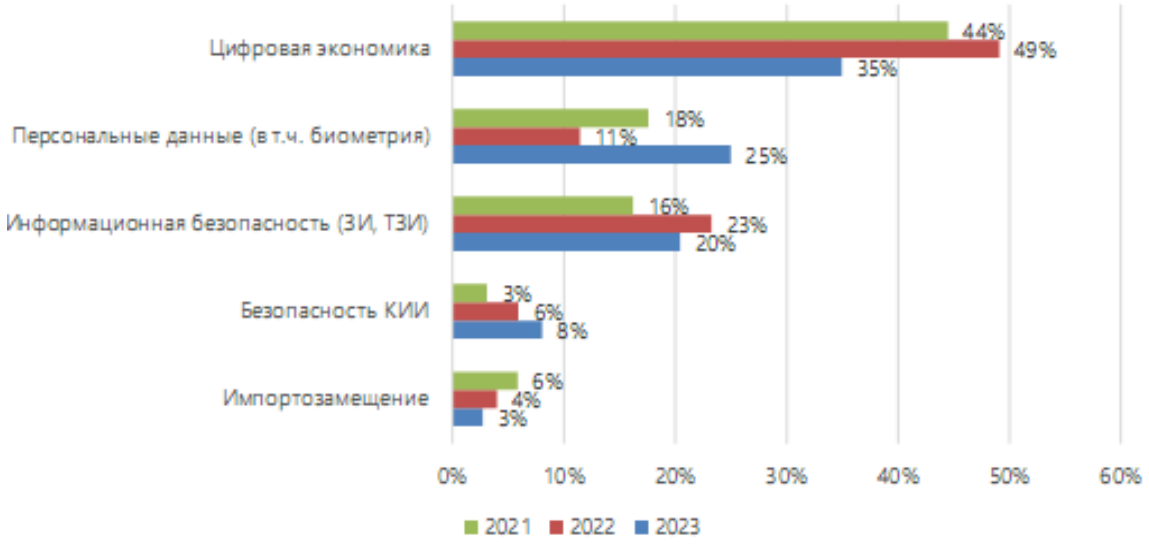

Рисунок 1.3 – Распределение документов по направлениям за 2021-2023 год (Источник: [63])

Таблица 1.2 – Группирование принятых документов и их проектов по направлениям (по данным Экспертно-аналитического центра InfoWatch [63])

Направления регулирования	Количественные показатели			Итого
	2021 г.	2022 г.	2023 г.	
1	2	3	4	5
Цифровизация	129	133	65	327
Системы защиты персональных данных	47	63	38	130
Информационная безопасность и защита информации	51	31	48	148
Безопасность инфраструктуры	9	16	16	41
Лицензирование	17	12	5	21
Импортозамещение	9	5	7	34
Нацбезопасность	12	5	4	21
Гостайна	6	3	1	12
Аккредитация	8	2	2	4
Сертификация	2	1	1	10
Итого:	290	271	187	748

б) правовая база профессиональных стандартов, например, профстандарты Минтруда России [64-70]:

- специалист по автоматизации информационно-аналитической деятельности;
- специалист по технической защите информации;
- специалист по безопасности компьютерных систем и сетей;
- специалист по защите информации в автоматизированных системах;
- специалист по защите информации в телекоммуникационных системах и сетях;
- специалист по информационным системам и другие;

в) ведомственную нормативную базу в сфере ИБ, например:

- регламенты (протоколы) информационно-технического (информационно-логического) взаимодействия между субъектами образовательной среды о компьютерных атаках на ведомственную информационную инфраструктуру;
- регламенты осуществления деятельности субъектов НОК ИБ в части обучения, подготовки, профессиональной подготовки и повышения квалификации специалистов, осуществляющих профессиональную деятельность в области ИБ;

Научно-техническое и учебно-методическое обеспечение содержит:

а) методы и способы выявления и предупреждения компьютерных инцидентов:

- методики (рекомендации) выявления признаков проведения компьютерных атак, определения их источников и способов осуществления и направленности;
- методики оценки степени защищенности информационных систем от компьютерных атак;
- методики обнаружения компьютерных атак на ведомственные информационные системы;

б) адаптированные нормативно-методические средства подготовки, переподготовки и повышения квалификации специалистов в области ИБ.

Ведомственная НОК ИБ *имеет этапы жизненного цикла* применительно к организационно-техническим системам, к регламентированным информационно-вычислительным системам, к системной инженерии и к процессам (процессам соглашения, организационного обеспечения, технического управления и техническим процессам) при декларировании «приспособленного соответствия» согласно приложения А ГОСТ Р 57193-2016 [71], с учетом регламентированной защиты информации для процесса управления по ГОСТ Р 59330-2021 [72]:

- *замысла* (потребности пользователей; образовательные процессы; перечень и качество предоставляемых сервисов);
- *разработки/производства* (способы и методы системотехнического построения; потребные технологии; выбор и отбор решений, в том числе готовых; верификация и валидация результатов);
- *эксплуатации* (внедрение, включая апробацию; сопровождение комплексов средств, баз данных и баз знаний, технологий, организационной и эксплуатационной документации; оценка результативности функционирования и качества образовательного процесса);
- *снятие с эксплуатации* (архивирование, хранение информационных ресурсов и персональных данных, утилизация).

Инфраструктурно ведомственная НОК ИБ развертывается поэтапно: от фрагмента до полномасштабной информационной инфраструктуры, взаимоувязано с ведомственными программными мероприятиями цифровой трансформации и цифрового развития.

Техническую основу развертывания НОК ИБ (первая очередь) должен составлять комплект средств ведомственного киберполигона на базе образовательной организации и ресурс ведомственной цифровой информационной инфраструктуры в интересах подготовки, переподготовки, повышения квалификации, тренировки и обеспечения информационной поддержки должностных лиц, осуществляющих профессиональную деятельность в области ИБ, территориальных органов ведомства и иных заинтересованных организаций.

Программные мероприятия учитывают:

- применение в качестве унифицированных платформенных решений результатов разработки (модернизации) СЗИ, технологических и информационных платформ различных производителей вне заказов ведомства, их верификацию и верификацию с обеспечением сервисов испытаний;
- разработку схемы территориально-распределенной инфраструктуры с возможностью ее представления в электронной форме в виде тематических слоев пространственных данных с возможностью оперативной актуализации данных;
- разработку регламентов обеспечения функционирования сервисов различных треков.

Комплектование сегментов, при необходимости, потребными сотрудниками (руководителями, ИТР, НПР) посредством перераспределения должностей (должностных обязанностей) в пределах штатной численности организаций, в интересах которых создан сегмент.

На первом этапе должен быть осуществлен ряд мероприятий:

- сформирован Пусковой комплекс первой очереди в составе функционального сегмента и сегмента управления;
- апробирован технический регламент оперативного взаимодействия субъектов;
- уточнена организационно-штатная структура службы эксплуатации сегмента управления;
- апробированы технологии трека образования и тестирования.

На втором этапе должны быть проведены следующие мероприятия:

- сформирован Пусковой комплекс второй очереди путем дооснащения функционального сегмента;
- ввод в действие схемы сочетания штатных и выделенных уполномоченных ресурсов сил и средств в интересах задач треков;
- ввод в действие штатного расписания сегмента управления.

На последующих этапах:

- во-первых, масштабируются системотехнические решения по построению сегментов, апробированные в функциональном сегменте в соответствии с планом развития;
- во-вторых, реализуются в полном объеме задачи и функции треков;

- в-третьих, осуществляется переход к сервис-ориентированной эксплуатации путем предоставления фиксированных и конструируемых информационно-функциональных услуг.

Планируется по образовательному треку на втором этапе выйти на реализацию сервисов в полном объеме. По треку кибертренировок ввести в постоянную практику образовательных дисциплин проведение кибертренировок в соответствии с фактическими условиями киберрисков на реальной ведомственной инфраструктуре. По треку испытаний целесообразно типизировать программы и методики испытаний.

2. Методология построения непрерывной образовательной среды информационной безопасности, интегрированной с ведомственной информационной инфраструктурой

Для организации НОК ИБ и защиты информации наблюдается тренд повсеместного создания и применения киберполигонов, который обусловлен руководящими документами и объективной необходимостью подготовки специалистов ИБ, организации и проведения испытаний в сфере ИБ. Основным методологическими подходами при этом являются методы программно-целевого развития организационно-технических систем [73]. Следует отметить, что ориентировочная стоимость только одной аппаратно-программной части киберполигона составляет десятки миллионов рублей. При этом остаётся актуальным ряд научно-практических вопросов:

- насколько эффективно киберполигон справляется с возложенными на него задачами;
- какие временные, финансовые, организационные, человеческие ресурсы требуются для полноценного функционирования;
- как киберполигон поведёт себя в условиях неопределённости и изменения объёма поставленных задач;
- сможет ли он выдержать реальные внешние кибератаки и достигать поставленных целей;
- где находятся пределы прочности киберполигона при увеличении нагрузки и другие аспекты.

Чтобы ответить на эти и другие подобные вопросы, необходимо системно подойти к проблематике анализа и синтеза киберполигона как организационно-технической системы.

По большей части организационно-технические системы класса киберполигон строятся посредством рационального обобщения опыта противостояния киберугрозам и создания такой инфраструктуры, которая позволяет испытать и выбрать лучшие практики, а также реализовать их в нужном контексте.

В работе [74] на основе анализа более 200 источников международная группа исследователей представила статистические данные эволюции предметной области киберполигонов и их онтологий с учетом распределения сфер применения, участников, используемых методов проведения киберучений/кибертренировок и реализуемых сценариев кибератак, архитектур построения, стеков протоколов и технологий виртуализации.

На Международном семинаре ESORICS 2023 International Workshops представлены материалы исследования [75] существующих зарубежных платформ для применения в качестве киберполигонов, адаптированных с учетом методов организации обучения и экспериментов, информационных инфраструктур и их топологий, а также возможного применения искусственного интеллекта для их конфигурирования под различные целевые задачи – как эволюционный путь развития платформ следующего поколения.

Подбор аналитического материала [76] по проблематике усовершенствований киберплощадок для прикладных задач киберфизических систем и информационных сетевых систем базируется на методологических рекомендациях поиска статей по определенным критериям и оценкам их качества (PRISMA) и анализе более чем 100 специализированных работ, на основании которых подтверждаются системные проблемы в архитектуре и инфраструктуре киберплощадок, что приводит к значительному росту нагрузки при админи-

стрировании и управлении предоставляемыми сервисами и формируемой требуемой конфигурацией.

Норвежскими специалистами в [77] рассмотрены различные аспекты разработки и оценки так называемых «неклассифицированных» киберполигонов (киберплощадок), которые в отличие от применяемых для обучения специалистов в области ИБ, привития навыков и повышения знаний о новейших киберугрозах, защите от них или смягчения последствий, предназначены для непрофильной аудитории с целью повышения их киберграмотности и киберкультуры (кибергигиены), в том числе для проведения тестирования безопасности.

Исследователи Чешского Университета им. Масарика (Брно) [78] представили отчет о десятилетнем опыте использования интеллектуального анализа данных поведенческих процессов участников киберучений/кибертренировок, таких как Capture the Flag (CTF) с применением технологий Domain-Driven Design для моделирования процесса подготовки специалистов на базе киберполигона с целью улучшить качество их подготовки. Вместе с тем, инфраструктурные аспекты киберполигона и проблематика организационной части остаются за рамками исследования.

В работе [79] обосновываются технические решения по созданию НОК ИБ с применением ведомственного киберполигона на основе анализа существующих практик создания подобных систем, зафиксированных в руководящих документах. Итоговое техническое решение выбирается экспертами с применением метода анализа иерархий. Такой подход обладает определенной долей субъективизма и предполагает некоторую статичность объекта управления с чётко заданными границами.

Исследование [80] посвящено выбору рационального варианта формирования инфраструктуры киберполигона как мультифункциональной инфраструктуры при существующих организационно-технических, финансовых и прочих ограничениях. Задача решается методом перебора всех возможных вариантов, каждый из которых характеризуется своим интегральным показателем эффективности. Предполагается: линейность системы управления; фиксированные границы системы; относительная стабильность структуры и функций киберполигона во времени.

Вместе с тем, синтез организационно-технических систем в условиях неопределённости изучался рядом авторов достаточно давно. Например, в работе [81] принято, что системы информационной безопасности в конкурирующих производственно-экономических структурах организационно включают в свой состав совокупность связанных единством цели элементов информационной безопасности (ИБ) на уровнях организационно-технических систем, технических систем и комплексов средств информационной безопасности. В работе упоминается, что синтез системы ИБ выполняется в условиях нечёткости и неопределённости исходных представлений о её задачах, составе, структуре и функционировании, при этом предполагаются фиксированные во времени границы системы и линейность системы управления, что является довольно сильным ограничением. По существу, сформулированная в исследовании задача решается методом последовательных приближений.

Более гибкое и менее формальное использования метода последовательных приближений для создания организационно-технических систем заложено в технологии Agile (гибкой разработки программного обеспечения), которая исследуется в работе [82], применительно к задачам формирования всестороннего организационного обеспечения вновь вводимых технологических систем компании. Авторы проинтервьюировали 52 респондента из Англии и Германии, выделили 4 модели компаний: бимодальная, полностью гибкая с межпродуктовой поддержкой, гибкая организация с проектной деятельностью, полностью гибкая организация без проектной деятельности; и 7 путей миграции компаний к полностью гибкой организации. Предлагаемый авторами подход учитывает неопределённость, с которой сталкивается компания, и позволяет управлять изменениями компании во времени, но слабо формализован

и, с точки зрения применимости к киберполигону, охватывает лишь часть киберполигона как объекта управления, в частности, только обеспечивающий уровень и уровень персонала согласно детализированной в [12] модели FIST (Full Infrastructure of Sources Toolkit), что является недостаточным для полного формирования системы.

Ещё одной группой вариантов синтеза системы управления организационно-техническими системами класса киберполигон или похожих на них путём последовательного приближения выступают технологии бизнес-моделирования: IDEF0, которая применена в [83] при формировании национальных систем наращивания потенциала в области кибербезопасности для стран с переходным этапом развития (NCCBF, National Cybersecurity Capacity Building Framework); BPM (Business Process Management), которая принята за основу в моделях жизненного цикла процессов [84] при персонализации киберучений; UML (Unified Modeling Language), которая применена в [85] для представления инновационных платформенных решений обеспечения кибербезопасности на основе моделей с проверкой полученных навыков обучающихся в рабочей среде (CYRA, CYber Range Assurance platform) и другие.

Синтез начинается с формализации показателей эффективности результирующей системы, затем так или иначе фиксируется точка зрения на систему (специалист информационной безопасности, управленец, пользователь системы и т.д.), после чего путём достаточного количества итераций, включающих в себя опрос специалистов, синтезируются функции и, возможно, некоторые элементы системы.

Эти технологии, в целом, позволяют учесть неопределённости в объекте управления, гибко изменять алгоритмы управления, однако есть ряд существенных недостатков:

во-первых, эффективность их применения существенно зависит от квалификации сотрудников, которые выполняют синтез;

во-вторых, фиксированные точки зрения дают несколько, порой не вполне связных между собой моделей системы, что порождает отдельную сложную задачу интеграции этих моделей в целостную модель;

в-третьих, переход от синтеза функций к синтезу структуры идёт интуитивно.

Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления ИБ, предложенная в [79], применяет декомпозицию на подграфы исходного графа организационного состава и структуры АСУ кибербезопасностью. При этом вопрос определения количества уровней в графе остаётся не решенным. В Методике принято, что структура и функции объекта управления и его элементов статичны.

В опубликованных работах не удалось обнаружить подходы, позволяющие найти и формализовать условие существования киберполигона как организационно-технической системы. Исключение составляет работа [86], где описывается метод iSOFT, позволяющий сформулировать условие, в понимании «обстоятельства» согласно словарю [87], существование системы, заданное в виде операторного уравнения. Когда получается найти такое условие, возможно синтезировать систему, которая гарантированно решает поставленные задачи.

Целью настоящего исследования является формулировка условия существования киберполигона как организационно-технической системы.

Под киберполигоном в настоящем исследовании понимается инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них, как определено в [88].

Следовательно, киберполигон должен за заданное время:

во-первых, формировать навыки и умения у заданного количества специалистов ИБ;

во-вторых, тестировать программное и аппаратное обеспечение в сфере ИБ.

Относительно ведомственного киберполигона конкретизация исходных данных формулируется следующим образом.

Киберполигон с учетом ведомственной специфики, представляет собой не просто виртуальную среду, а единую организационно-техническую систему, состоящую из территориально-распределенных сегментов сил и средств, объединенных цифровой сетью связи, с централизованным управлением на базе ведомственной образовательной организации.

Ключевые особенности ведомственного киберполигона:

- ведомственная принадлежность: киберполигон предназначен для решения задач, связанных с обеспечением ИБ МЧС России, с учетом специфики деятельности ведомства и решаемых задач;
- многофункциональность: киберполигон объединяет несколько треков, каждый из которых направлен на решение определенных задач:
- образовательный трек: предметно-ориентированное обучение и повышение квалификации специалистов по ИБ, интегрированное с электронной информационно-образовательной средой вузов МЧС России;
- трек киберучений: организация киберучений, тренировок и соревнований для специалистов ИБ и руководителей (должностных лиц);
- трек исследований и тестирования: апробация и тестирование новых технологий и средств защиты информации, исследование проблемных вопросов кибербезопасности, наполнение банка данных угроз ФСТЭК России;
- территориальная распределенность: киберполигон состоит из сегмента с функциями управления и территориальных сегментов, развернутых в различных подразделениях ведомства;
- интеграция с ведомственной информационной инфраструктурой: киберполигон должен быть интегрирован с действующими системами (СЭД, КС АРМ ГС, ЕДДС АИУС РСЧС и т.д.), а также иметь возможность взаимодействия с внешними системами, например, ГосСОПКА;
- оперирование пространственными данными (данными о пространственных объектах и их наборах): расположение оборудования, объектов критической информационной инфраструктуры, геолокация пользователей и пр., следовательно, информационная система в основе киберполигона является геоинформационной системой в терминах ГОСТ Р 52155-2003;
- масштабируемость и развиваемость: киберполигон должен обеспечивать возможность поэтапного наращивания мощностей, добавления новых функций, модернизации и адаптации к новым задачам и угрозам.

Таким образом, в киберполигоне МЧС России присутствует несколько явно выраженных уровней, связанных с документальным сопровождением, работы персонала и аппаратно-программных средств, взаимодействие которых рассматривается в модели *FIST*.

Киберполигон МЧС России представляет собой сложную организационно-техническую систему, включающую в себя не только программное и аппаратное обеспечение, но и персонал, пользователей, нормативно-правовые документы, финансовые потоки и другие взаимосвязанные элементы. Традиционные исследования информационной безопасности рассматривают эти элементы изолированно, упуская из виду их взаимосвязь и влияние друг на друга, что усложняет формализацию условия существования киберполигона, то есть условия, выполняя которое, киберполигон гарантированно достигает своей цели деятельности.

Модель *FIST* (*Full Infrastructure of Sources Toolkit*) [12] позволяет рассмотреть киберполигон как иерархическую систему с обеспечивающим уровнем, уровнем персонала, уровнями аппаратного и программного обеспечения (см. рисунок 2.1).

Метауровни задают требуемые пространственно-временные состояния вложенных уровней, например: руководящие документы содержат требования к персоналу, аппаратно-

программному обеспечению; персонал настраивает и обеспечивает функционирование аппаратно-программного обеспечения; аппаратура предоставляет заданные ресурсы программному обеспечению.

От вложенных уровней в сторону метауровней идёт обратная связь, например: выбранное программное обеспечение не позволяет организовать многопользовательскую подготовку специалистов ИБ, распределённых в пространстве времени, что может потребовать применения распределённого в пространстве-времени аппаратного обеспечения, что в свою очередь изменяет требования к обслуживающему персоналу, что влечёт за собой изменения в руководящих документах или финансовом обеспечении.

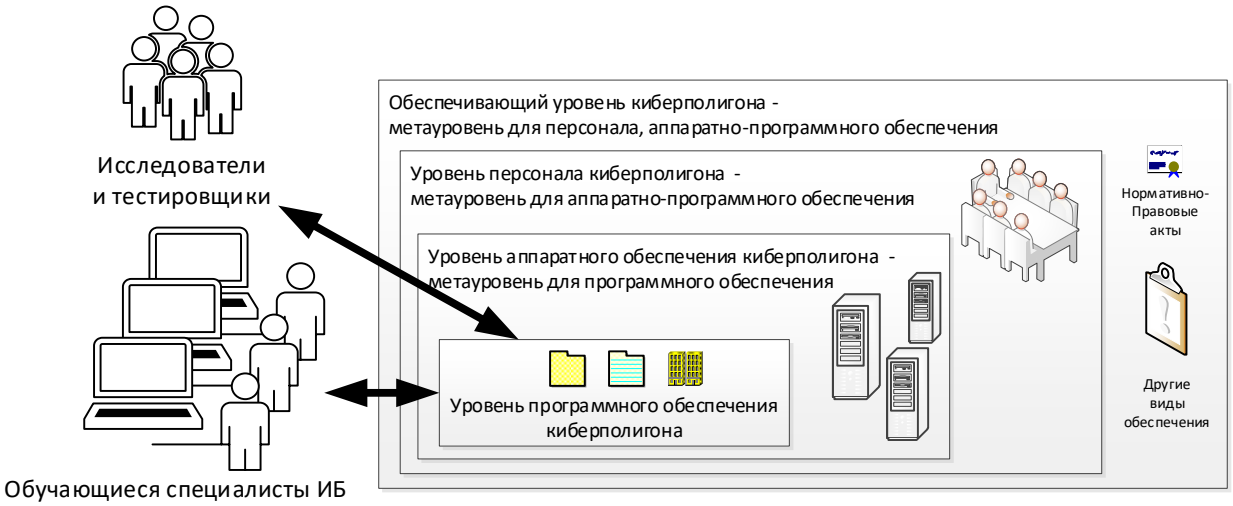

Рисунок 2.1 – Киберполигон согласно модели FIST

Киберполигон существует на всех уровнях модели FIST:

а) во-первых, на обеспечивающем уровне:

- в виде нормативно-правового обеспечения – регламентов, политик, распоряжений и т.д.;
- как система, оперирующая с финансовыми средствами;
- содержит регламентированные профессиональные требования к специалистам ИБ, мотивационные и воспитательные составляющие;

б) во-вторых, на уровне персонала в качестве преподавателей и вспомогательного персонала;

в) в-третьих, на аппаратном уровне как оборудование, на котором развёрнуто программное обеспечение, необходимое для жизнедеятельности киберполигона;

г) в-четвертых, на уровне программного обеспечения как набор специальных и общесистемных программ, с использованием которых:

- осуществляется непосредственная подготовка специалистов ИБ;
- выполняются действия, обеспечивающие работу киберполигона: бухгалтерия, кадры, резервное копирование и пр.

Уровни непрерывно взаимодействуют между собой и ориентированы на достижение цели деятельности всего киберполигона, и значит, система, синтезированная с использованием модели *FIST*, является целостной [45].

Множество пространственно-временных состояний киберполигона S состоит из множеств пространственно-временных состояний каждого уровня.

$$S = S^E \cup S^P \cup S^{Hard} \cup S^{Soft}, \quad (2.1)$$

где S^E – множество пространственно-временных состояний обеспечивающего уровня;

S^P – множество пространственно-временных состояний уровня персонала;

S^{Hard} – множество пространственно-временных состояний уровня аппаратного обеспечения;

S^{Soft} – множество пространственно-временных состояний уровня программного обеспечения.

Пространственно-временное состояние системы – это сложившиеся отношения между элементами системы на момент времени.

Киберполигон предназначен для решения задач по подготовке специалистов ИБ (*e*, *education*) и для проведения испытаний в сфере ИБ (*test*, *testbeds*). Значит, можно сказать, что он обладает производительностью

$$\Omega_{CR} = \{\Omega_e, \Omega_{test}\}, \quad (2.2)$$

где Ω_e – производительность киберполигона по подготовке специалистов ИБ: количество специалистов в единицу времени;

Ω_{test} – производительность киберполигона по проведению испытаний: количество испытаний в единицу времени.

Производительность (Ω) – количество задач $|K|$, решённое за время t:

$$\Omega=|K|/t, \quad (2.3)$$

где K – множество решаемых задач.

Множество задач K^*, которые должен решить киберполигон, определяется метасистемой-заказчиком, то есть задаётся извне.

Производительность всего киберполигона зависит от производительности каждого уровня киберполигона, от того, насколько элементы согласованы между собой:

$$\Omega_{CR} = F_{\Omega}(\Omega^E, \Omega^P, \Omega^{Hard}, \Omega^{Soft}, S, T), \quad (2.4)$$

где Ω^E – производительность обеспечивающего уровня: скорость разработки нормативно-правовых документов, срок действия документов, объём финансирования в единицу времени и т.д.;

Ω^P – производительность уровня персонала: количество задач, решаемых персоналом в единицу времени, «время жизни» персонала и т.д.;

Ω^{Hard} – производительность уровня аппаратного обеспечения: *MIPS*, *FLOPS*, бод и т.д.;

Ω^{Soft} – производительность уровня программного обеспечения: скорость сходимости реализованных алгоритмов, вычислительная сложность алгоритмов, ресурсоёмкость применяемых команд и т.д.;

T – множество моментов времени, в которые функционирует киберполигон.

Среда, воздействие которой обрабатывает киберполигон, имеет различную природу [89, 90]:

во-первых, детерминированная среда (Q_d), воздействие которой известно заранее и может быть описано аналитически: техническое обслуживание, расписание подготовки специалистов ИБ, проведения испытаний и т.д.;

во-вторых, стохастическая среда (Q_{st}), воздействие которой на систему выбирается из *известного множества альтернатив* случайным образом *при полностью известном вероятностном описании «механизма» этого выбора*: естественные сбои и отказы, поток задач, согласованных с метасистемой-заказчиком и т.д.;

в-третьих, среда нестохастическая (Q_{nst}), то есть среда, которая не является средой Q_d и Q_{st}. Эта среда характеризуется тем, что:

а) воздействие на киберполигон выбирается из известного множества альтернатив согласно некоторой цели либо отсутствуют некоторые элементы вероятностного описания «механизма» выбора;

б) воздействие на киберполигон не описывается в рамках других сред:

- новые неучтённые ранее задачи, поставленные метасистемой-заказчиком;

- новая активность злоумышленников. Формализация подобных целенаправленных агрессивных действий требует применения нестохастических моделей, позволяющих адекватно оценить возможности атакующей стороны [89];
- изменения в ландшафте киберугроз и пр.

Назначение киберполигона – тренировать специалистов ИБ, которые и атакуют инфраструктуру, и защищают её. Специалисты ИБ должны иметь актуальные навыки в сфере ИБ, то есть деятельности, которая сильно и непредсказуемо изменчива.

Следовательно, киберполигон:

- функционирует в условиях изменчивости цели управления: нужно готовить требуемое количество специалистов ИБ с актуальными знаниями, при этом требуемое количество специалистов и актуальность знаний изменчива;
- поскольку киберполигон имеет ведомственную принадлежность с некоторой автономией на местах, то управление им будет сочетать в себе элементы и централизации, и самоорганизации;
- архитектура киберполигона в виде совокупности структуры и протоколов взаимодействия элементов структуры между собой и со средой практически непрерывно изменяется в пространстве-времени;
- имеет тенденцию саморазрушаться, что является штатным режимом функционирования и должно учитываться управляющей системой. Для компенсации такой деградации могут применяться методики, использующие внутренние резервы решаемых задач, такие как допустимые погрешности и временные лаги, что позволяет снизить требования к производительности системы в условиях деструктивных воздействий [91];
- может подвергаться нестохастическим воздействиям внешних систем: кибератаки, резкое изменение требований к количеству и качеству подготавливаемых специалистов ИБ, появление новых угроз и т.д.

Таким образом, киберполигон представляет собой объект изменяющейся целью управления, с динамично изменяемой архитектурой, функционирующий в среде всех возможных типов, и значит, целесообразно его рассматривать как адаптивную систему управления.

Система управления – это сочетание управляющей системы и объекта управления [92].

Операторное уравнение, описывающее работу системы управления киберполигоном

Цель управления киберполигоном – решить множество поставленных задач $\boldsymbol{K}^*$ за заданное время t, несмотря на воздействия окружающей среды и саморазрушение киберполигона.

Следовательно, должна быть разработана система показателей, описывающая насколько киберполигон способен достичь своей цели деятельности.

Решить проблему управления – решить проблему выбора из множества альтернатив [30].

$$\{U_{\text{доп}}, S\} \to U_{sat}, \tag{2.5}$$

где $U_{\text{доп}}$ – множество допустимых управляющих воздействий;

U_{sat} – множество управляющих воздействий, реализующих сатисфакционное управление киберполигоном и адаптирующих киберполигон к обработке входящих воздействий.

Киберполигон является децентрализованной системой, распределённой в пространстве-времени, следовательно, в произвольное время к киберполигону подключаются или отключаются от него сегменты с разными наборами управляющих воздействий.

Это означает, что множество допустимых управляющих воздействий $\mathbf{U}_{\text{доп}}$ изменяется во времени.

Задача управления может быть упрощена, если потребовать неизменность $\mathbf{U}_{\text{доп}}$. Физически неизменность реализуется разработкой соответствующих регламентов и созданием на устройствах специальной среды для решения задач киберполигона: виртуальная машина, контейнер или какой-то другой вариант виртуализации.

Ограничение 1. Множество $U_{\text{доп}}$ неизменно во все моменты времени из множества T.

Согласно работе [94] в ходе адаптации необходимо определить объект управления. Это означает, что задача адаптивного управления распадается на две крупные части [93]:

- идентификация объекта управления, то есть наблюдение;
- выбор управляющего воздействия.

Следовательно, модель киберполигона примет вид, приведенный на рисунок 2.2.

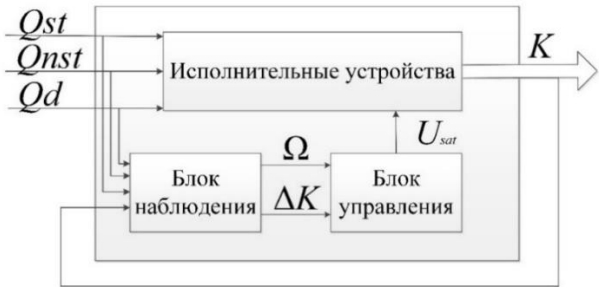

Рисунок 2.2 – Модель киберполигона с блоком наблюдения и управления

Согласно предложенной модели, наблюдение и управление киберполигоном реализуются через производительности. Интегральная производительность формируется через оптимизацию структуры киберполигона и оптимизацию процессов выполнения задач.

Таким образом, проблема адаптации киберполигона к обработке входящих воздействий формулируется так.

Дано:

T – множество моментов времени, когда функционирует киберполигон;

$Q=\{Q_d, Q_{st}, Q_{nst}\}$ – множество входных ситуаций;

$\Omega_{CR} = F_\Omega(\Omega^E, \Omega^P, \Omega^{Hard}, \Omega^{Soft}, S, T)$ – производительность киберполигона;

$K^* = \bigcup_{i=1}^{|K^*|} k_i, k_i = \langle \Omega^*_{CR,i}, t^*_i \rangle$ – множество поставленных задач;

t^*_i – требуемое время решения i-ой задачи;

$\Omega^*_{CR,i}$ – производительность киберполигона, которая требуется i-ой задаче;

$U_{доп}$ – множество управляющих воздействий.

Ограничение 2. $t_i \ll \tau, \forall i = \overline{1, |K^*|}$, τ – среднее время стабильного существования киберполигона.

Требуется:

При фиксированном $\boldsymbol{U}_{доп}$ найти такое управляющее воздействие $\boldsymbol{U}_{sat} \subset \boldsymbol{U}_{доп}$, которое позволит решить все задачи, поставленные перед киберполигоном за заданное время, то есть найти оператор:

$$R_U(\Omega_{CR}, Q, U_{sat}, T) = K^*. \quad (2.6)$$

Операторное уравнение (2.6) является моделью системы адаптивного управления киберполигоном и реализует условие адаптации киберполигона к обработке входящих воздействий, то есть условие гарантированного решения киберполигоном поставленных задач. При создании уравнения используются все возможные субстанциальные закономерности киберполигона, то есть закономерности, которые влияют на достижение системой цели её деятельности [95].

Решение операторного уравнения (2.6) представляет собой вариационную задачу, так одно уравнение содержит несколько переменных.

Из представленной модели следует, что множество задач K, которые решает киберполигон, может не совпадать со множеством задач K^*, поставленных метасистемой-заказчиком перед киберполигоном. Так происходит в следующих случаях:

- киберполигон решает меньше задач, чем поставили, потому что не справляется с нагрузкой в силу резкого увеличения задач или своего разрушения из-за кибератак или в ходе эксплуатации;

- киберполигон решает задачи злоумышленников.

Пример применения разработанной модели.

Без нарушения общности предположим, что перед киберполигоном стоит задача повышать квалификацию 10 специалистам ИБ в месяц:

$\Omega_{CR} = \Omega_e = 10$ специалистов в месяц на протяжении года.

Киберполигон функционирует T = 1 год = 12 месяцев.

k^* – подготовить 10 специалистов ИБ.

$|K^*| = 12$, так как всего 12 задач (10 специалистов каждый месяц на протяжении года).

$$K^* = \bigcup_{i=1}^{12} k_i \,, k_i = \langle \Omega^*_{CR,i} = 10, t^*_i = 1 \rangle. \quad (2.7)$$

Q_{st} = равномерное появление 14+-5 специалистов ИБ в месяц желающих повысить свою квалификации.

Q_{nst} = текущая ситуация в сфере ИБ, которая влияет на формирование перечня требований к специалисту ИБ. Может изменяться раз в неделю.

Исходя из условий примера, можно сказать, что:

- киберполигон должен содержать какой-то элемент, который преобразует стохастическую величину на входе Q_{st} в детерминированную Ω_{CR} на выходе, например, за счёт управления количеством обучающихся в группе;
- полностью формировать перечень требований к специалистам ИБ на уровне руководства МЧС нецелесообразно, потому что текущая ситуация в сфере ИБ Q_{nst}, влияющая на формирование требований, изменяется раз в неделю, что гораздо быстрее, чем формируются и утверждаются локальные нормативные акты, например в МЧС России (больше года, то есть 52 недели). Следовательно, частично требования к специалисту ИБ необходимо формировать в ходе самого обучения;
- среднее время стабильного существования киберполигона должно быть много больше одного месяца.

Конкретный вид оператора (2.6) и его составляющих определяется на стадиях 4 «Эскизный проект» и 5 «Технический проект» по ГОСТ Р 59793-2021 создания автоматизированных систем и реализуется методом *iSOFT*.

Поскольку оператор строится с использованием *всех* субстанциальных закономерностей, то пригодность и адекватность модели обеспечивается полнотой учёта закономерностей.

3. Технология построения непрерывной образовательной среды информационной безопасности, интегрированной с ведомственной информационной инфраструктурой

Предложенная методология построения НОК ИБ, интегрированной с ведомственной информационной инфраструктурой, на основе операторного уравнения задает общие условия существования и адаптации киберполигона как организационно-технической системы.

Для практической реализации этих условий и перехода к проектированию конкретных структур и процессов разработана технология построения, основанная на онтологическом моделировании бизнес-процессов. Технология позволяет декомпозировать общую задачу управления, выраженную оператором F, на конкретные процедуры синтеза организационной и технической структур, обеспечивая тем самым выполнение заданных требований к производительности (Ω) и составу решаемых задач (K).

Общий методологический подход к выбору системотехнических решений построения технологической части организационно-технической системы (ОТС) класса «киберполигон» как информационно-технической системы (ИТКС), представленный на рисунке 3.1, учитывает их особенности, принципы и условия построения [79, 33].

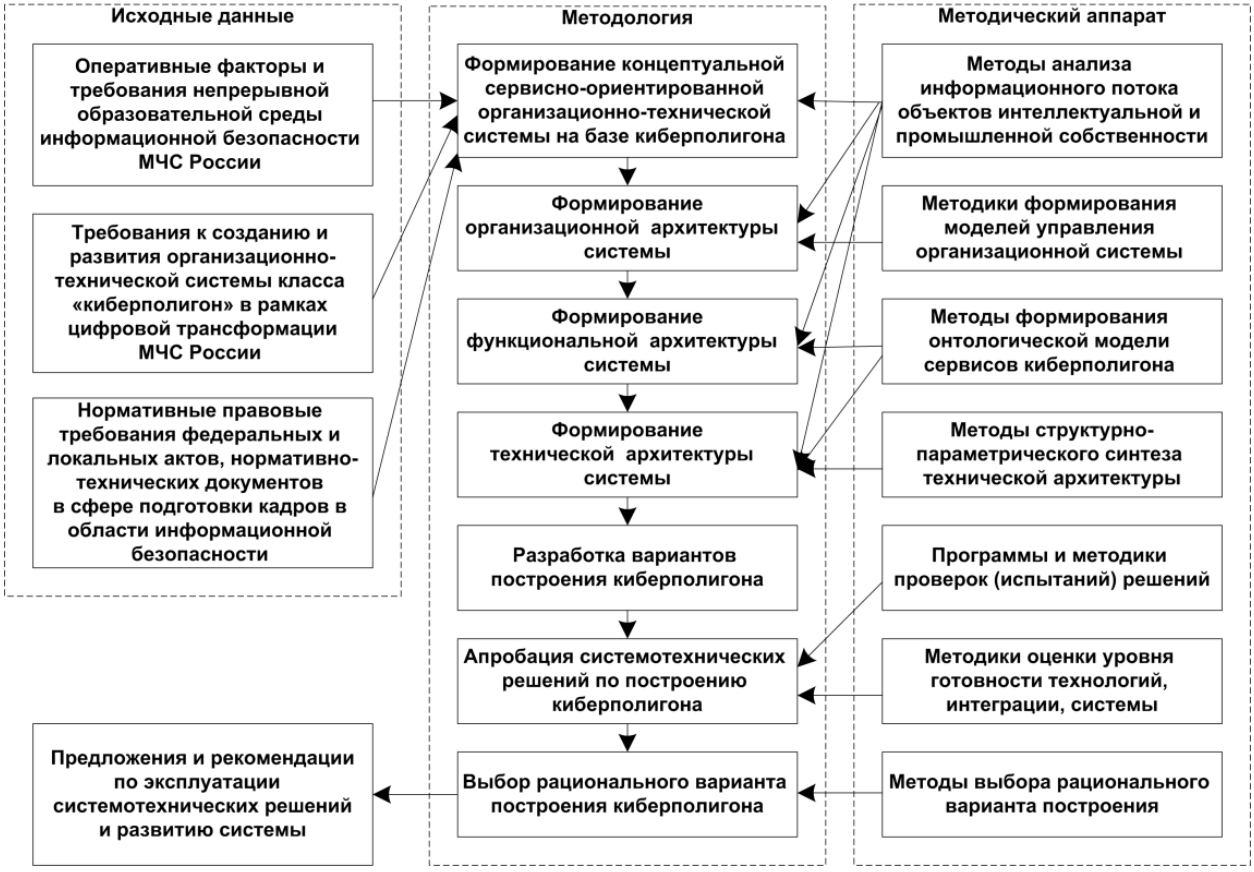

Рисунок 3.1 – Методологический подход к выбору ОТС класса «киберполигон»

Формальная постановка задачи управления ОТС класса «киберполигон» проведена на основе анализа современных методологических подходов к управлению в ОТС [79, 33].

В исследовании принято, что ОТС класса «киберполигон» определена на трехкомпонентной структуре управления в организационной системе типа:

<Центр> – <Агент> – <Управляемый объект>,

которая представлена иерархически взаимоувязанной совокупностью соответствующих моделей принятия решений, действий, результатов (u, y, z) деятельности (рисунок 3.2).

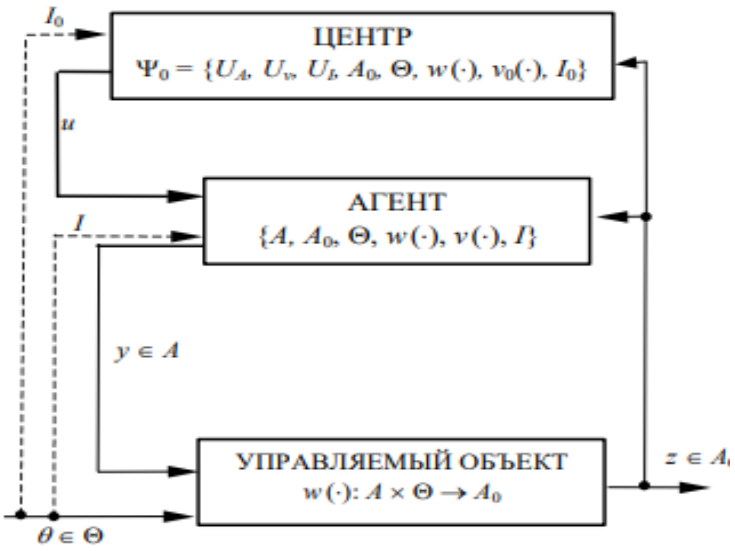

Рисунок 3.2 – Модель управления в 3-х уровневой организационной системе [79, 33]

Пусть модель принятия решений подсистемой «Центр» (как модель ведомственной подсистемы управления СОИБ в части потребности в сервисах треков киберполигона) описывается кортежем:

$$\Psi_0 = \{U_A, U_v, U_I, A_0, \Theta, w(\cdot), v_0(\cdot), I_0\}, \quad (3.1)$$

при $u = (u_A, u_v, u_I) \in U$; $U = U_A \times U_v \times U_I$,

где u_A, u_v, u_I – стратегии институционального, мотивационного и информационного управления Центра $u_A \in U_A$, $u_v \in U_v$, $u_I \in U_I$; U_A, U_v, U_I, – множество стратегий институционального, мотивационного, информационного управления (нижние индексы в обозначениях соответственно) Центра (ведомственной СОИБ); U – вектор управлений Центра; $v_0(\cdot)$ – предпочтения Центра.

Тогда, задача управления ОТС класса «киберполигон» с учетом стратегии информационного управления Центра (u_I) формулируется следующим образом: найти допустимое управляющее воздействие, имеющее максимальную эффективность (оптимальное управление) [79, 33]

$$K(u) \to \max_{u \in U} \quad (3.2)$$

при ограничениях на реализацию стратегий институционального (u_A) и мотивационного (u_v): $u_A \in \varnothing$; $u_v \in \varnothing$.

Результаты анализа существующего методического аппарата управления в организационных системах близкой проблематики выявили необходимость постановки частных научных задач с учетом следующих ограничений и допущений: организационная структура ведомственной СОИБ – типовая; силы и средства СОИБ – в пределах штатной численности; режим функционирования СОИБ – повседневная деятельность.

Киберполигоны на современном этапе развития СОИБ являются достаточно новым классом организационных систем с собственной ИИ на основе информационно-коммуникационных и ИБ-технологий в подсистемах поддержки принятия решений метасистем, обеспечивающие решение задач обучения (подготовки) ДЛ в области ИБ.

Интенсивные научные исследования и результаты практической реализации сфокусированы по направлениям развития уровня агрегирования технологий, целям использования и эффективности интеграции компонент СОИБ с реальными бизнес-процессами и бизнес-задачами различных секторов экономики.

Адаптировать имеющиеся прототипированные решения киберполигонов в метасистемы различного назначения без унифицированных подходов к их проектированию, концептуального моделирования и оценки полученных решений практически невозможно.

В рамках выполнения настоящей НИР опубликована работа [33], в которой сформулирована и решена задача онтологического описания ведомственного киберполигона на основе модели eTOM бизнес-телекома, регламентированной международными и национальными стандартами, в постановке:

$$G^{eTOM} \xrightarrow[P_{КП}^{eTOM}]{} G_{КП}^{eTOM} \xrightarrow[P_{КП}^{O}]{} G_{КП}^{O} \quad (3.3)$$

где $G_{КП}^{eTOM}$ – граф процессов деятельности КП; $G_{КП}^{O}$ – граф онтологии КП; $P_{КП}^{eTOM}$, $P_{КП}^{O}$ – функции преобразования графов процессов eTOM и онтологии (О) применительно к КП.

Онтологическая модель КП является информационно-логической (математической) моделью структуризации бизнес-процессов организационной системы под задачи ведомственной СОИБ, формирования в трехкомпонентной системе управления требуемых стратегий управления в организационной системе на уровне Центра u ($u = u_I$; $u \in U_I$), набора соответствующих действий управления в организационной системе (подсистеме управления КП) на уровне Агента y ($y \in A$) и требуемых результатов деятельности в организационной системе (подсистеме формирования сервисов треков, эксплуатации и обеспечения) на уровне Управляемого объекта z ($z \in A_0$) [79, 33].

Методика формирования онтографа киберполигона представлена блок-схемой на рисунке 3.3, а содержательное формирование модели в таблицах 3.1-3.3.

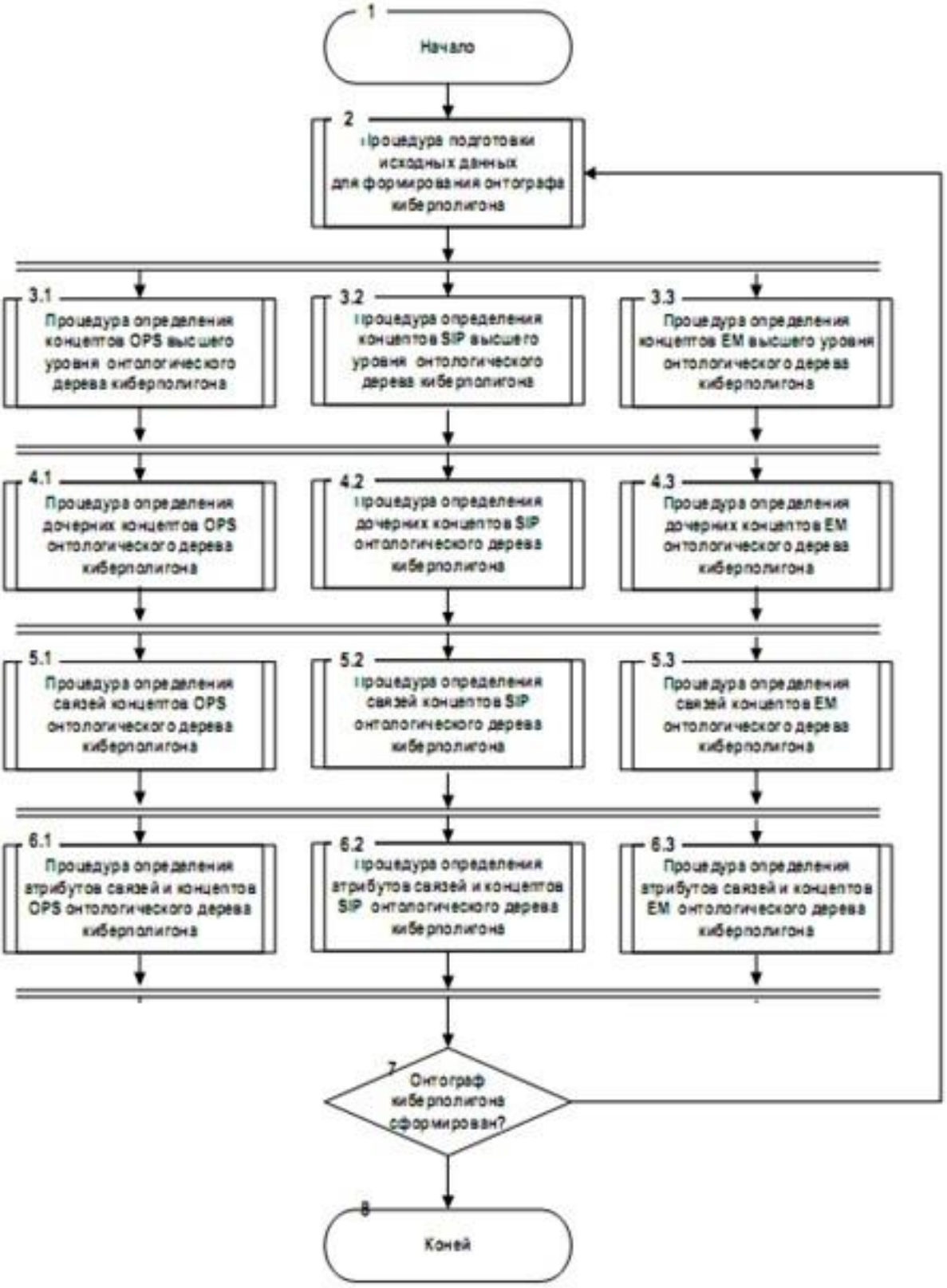

Рисунок 3.3 – Блок-схема формирования онтографа киберполигона

Таблица 3.1 – Результаты формирования концептов областей онтографа (фрагмент, область OPS)

Главные области	Концепты высшего уровня (по трекам киберполигона)		
	сервисы ОТ	сервисы КТ	сервисы ИТ
1	2	3	4
$G^{eTOM}_{OPS,КП}$	1. Управление интерфейсами с клиентами (1.1.1.2) 2. Конфигурирование и активация услуг (1.1.2.2) 3. Управление качеством услуг (1.1.2.4) 4. Управление параметрами работы ресурсов (1.1.3.4) 5. Сбор и распределение данных о ресурсах (1.1.3.5) 6. Подготовка ресурсов (1.1.3.2) 7. Поддержка и обеспечение готовности процессов групп 1-4 (1.1.1.1–1.1.4.1) 8. Обработка проблем клиентов (1.1.1.6) 9. Управление разрешением проблем с услугами (1.1.2.3) 10. Управление авариями на ресурсах (1.1.3.3)	1. Управление интерфейсами с клиентами (1.1.1.2) 2. Конфигурирование и активация услуг (1.1.2.2) 3. Управление качеством услуг (1.1.2.4) 4. Управление параметрами работы ресурсов (1.1.3.4) 5. Сбор и распределение данных о ресурсах (1.1.3.5) 6. Подготовка ресурсов (1.1.3.2) 7. Поддержка и обеспечение готовности процессов групп 1-4 (1.1.1.1–1.1.4.1)	1. Управление параметрами работы ресурсов (1.1.3.4) 2. Управление параметрами работы с помощью поставщиков и партнеров (1.1.4.4) 3. Сбор и распределение данных о ресурсах (1.1.3.5) 4. Управление заказами на продукцию поставщиков и партнеров (1.1.4.2) 5. Поддержка и обеспечение готовности процессов групп 1-4 (1.1.1.1–1.1.4.1)
$G^{eTOM}_{SIP,КП}$	1. Разработка и управление услугами (1.2.2)	1. Разработка и управление услугами (1.2.2)	1. Разработка и управление цепочками поставок (1.2.3)
$G^{eTOM}_{EM,КП}$	1. Управление отношениями с заинтересованными сторонами и внешними связями (1.3.6)	1. Управление отношениями с заинтересованными сторонами и внешними связями (1.3.6)	1. Управление знаниями организации и исследованиями (1.3.4) 2. Управление отношениями с заинтересованными сторонами и внешними связями (1.3.6)

Таблица 3.2 – Отношения между концептами высшего уровня онтологической модели киберполигона (главная область OPS, пример)

Треки КП	Отношения между концептами высшего уровня		
	вертикальные	горизонтальные	между областями
1	2	3	4
ОТ	Выполнение заказов Обеспечение качества Поддержка и обеспечение готовности процессов	Управление взаимоотношениями с клиентами (1.1.1) Управление и эксплуатация услуг (1.1.2) Управление и эксплуатация ресурсов (1.1.3)	Разработка и управление ресурсами
КТ	Выполнение заказов Обеспечение качества Поддержка и обеспечение готовности процессов	Управление взаимоотношениями с клиентами (1.1.1) Управление и эксплуатация услуг (1.1.2) Управление и эксплуатация ресурсов (1.1.3)	Разработка и управление ресурсами
ИТ	Обеспечение качества Поддержка и обеспечение готовности процессов	Управление и эксплуатация услуг (1.1.2) Управление взаимоотношениями с поставщиками и партнерами (1.1.4)	Разработка и управление услугами Разработка и управление цепочками поставок

Таблица 3.3 – Аксиоматика концептов высшего уровня и отношений онтологической модели киберполигона (главная область EM, пример)

Треки КП	Аксиоматика концептов высшего уровня и отношений	
	концептов	отношений
1	2	3
ОТ КТ	Концепты ОТ и КТ для классификации процессов организационно-технической системы, а не моделирования реальных процессов.	Отношения между концептами ОТ и КТ от начального процесса OPS "Управления взаимоотношениями с клиентами" (1.1.1)
ИТ	Концепты ОТ, КТ и ИТ ориентированы на корпоративные связи	
	Концепты ИТ для обеспечения персонала киберполигона необходимыми знаниями и определения приоритетов НИОКР в интересах организации с оценкой технологий и их поставщиков	Отношения между концептами ИТ для потоковых диаграмм реальных процессов по управлению знаниями организации и управлению исследовательскими работами

Определение и оценка возможностей программных (программно-аппаратных, аппаратно-программных) средств при использовании в КП ведомственного назначения могут быть проведены на основе системы критериев, представленных на рисунке 3.4.

Рисунок 3.4 – Уточненная классификация критериев качества решений применительно к организационным системам класса «киберполигон»

Адекватность разработанной онтологической модели процессов управления в ОТС класса «киберполигон» (далее – Модель 1) по отношению к организационной структуре ведомственной типовой СОИБ и организационной структуре концептуальной модели КП ведомственного назначения проверялась экспертным методом оценки значений показателей ее характеристик с инфологическими моделями процессов управления известных прототипов (Модели 2-5), как показано в работе [80].

Результаты оценки адекватности онтологических моделей процессов управления для ОТС класса «киберполигон» представлены в таблице 3.4

Достоверность разработанной онтологической модели процессов управления для ОТС класса «киберполигон» подтверждается отображением компонент КП и процессов управления в организационных системах с применением ERwin-средств.

Пример процессного описания сервисов ОТ ведомственного КП с использованием ERwin-средств представлен на рисунке 3.5.

Таблица 3.4 – Аксиоматика концептов высшего уровня и отношений онтологической модели киберполигона (главная область ЕМ, пример)

Перечень свойств и характеристик модели	Значения показателей характеристик онтологических моделей				
	1	2	3	4	5
1. Полнота учета сервисов КТ киберполигона	Полном объеме	Полном объеме	Частично	Полном объеме	Частично
2. Полнота учета сервисов ОТ киберполигона	Полном объеме	Полном объеме	Частично	Полном объеме	Частично
3. Полнота учета сервисов ИТ киберполигона	Полном объеме	Полном объеме	Частично	Полном объеме	Частично
4. Полнота учета сервисов внешнего взаимодействия	Полном объеме	Полном объеме	Значительно	Полном объеме	Частично
5. Детализация стратегий СОИБ по управлению КП	Значительно	Нет	Нет	Нет	Частично
6. Детализация действий управления в КП	Полном объеме	Полном объеме	Полном объеме	Значительно	Частично
7. Детализация результатов деятельности по управлению в КП	Полном объеме	Полном объеме	Значительно	Значительно	Частично
8. Гармонизация компонент модели с отечественной нормативно-правовой базой управления в организационных системах	Полном объеме	Полном объеме	Полном объеме	Значительно	Значительно
9. Соответствие организационной структуре ведомственных СОИБ	Значительно	Нет	Частично	Значительно	Частично
10. Соответствие организационной структуре ОТС класса «киберполигон»	Полном объеме	Частично	Частично	Значительно	Полном объеме
11. Соответствие организационной структуре подсистемы управления ОТС класса «киберполигон»	Полном объеме	Частично	Значительно	Значительно	Полном объеме
12. Соответствие оргструктуре управления подсистемы предоставления сервисов, эксплуатации, технического обеспечения и развития	Полном объеме	Частично	Значительно	Значительно	Полном объеме

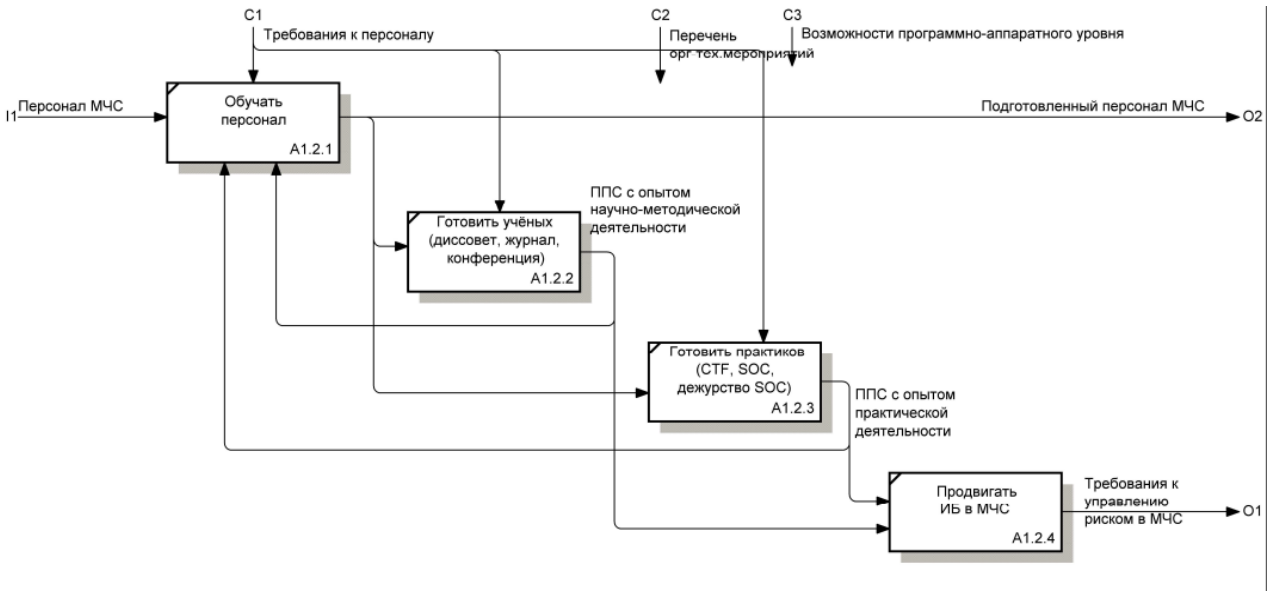

Рисунок 3.5 – Реализуемость процессного описания (фрагмент)

Результаты оценок качества решений построения киберполигона представлены на рисунке 3.6.

В работах [79, 33] представлены результаты разработки комплексной методики синтеза организационно-технических структур ОТС класса «киберполигон» ведомственного назначения.

Комплексная методика синтеза организационно-технических структур класса «киберполигон» предназначена для формирования научно-обоснованных системотехнических решений, их рационального построения и управления сервисами в интересах ведомственных СОИБ.

Перечень свойств среды оценки	Значение показателей
1. Уровень реализации задач	В полном объеме
2. Уровень доступности результатов	В полном объеме
3. Уровень зрелости системы	В полном объеме
4. Уровень объекта техники	В полном объеме
5. Уровень регламентированных решений	Значительно
6. Уровень системной и программной инженерии	В полном объеме
7. Уровень отраслевой реализуемости	Значительно
8. Уровень реализуемости образовательной среды	В полном объеме

Рисунок 3.6 – Результаты оценок качества решений построения киберполигона

Методикой предусматривается технико-экономическая оценка, которая реализуется в процедуре выбора рационального варианта построения архитектуры КП с учетом этапности ее формирования.

Структура предлагаемой комплексной методики представлена в виде блок-схемы на рисунке 3.7.

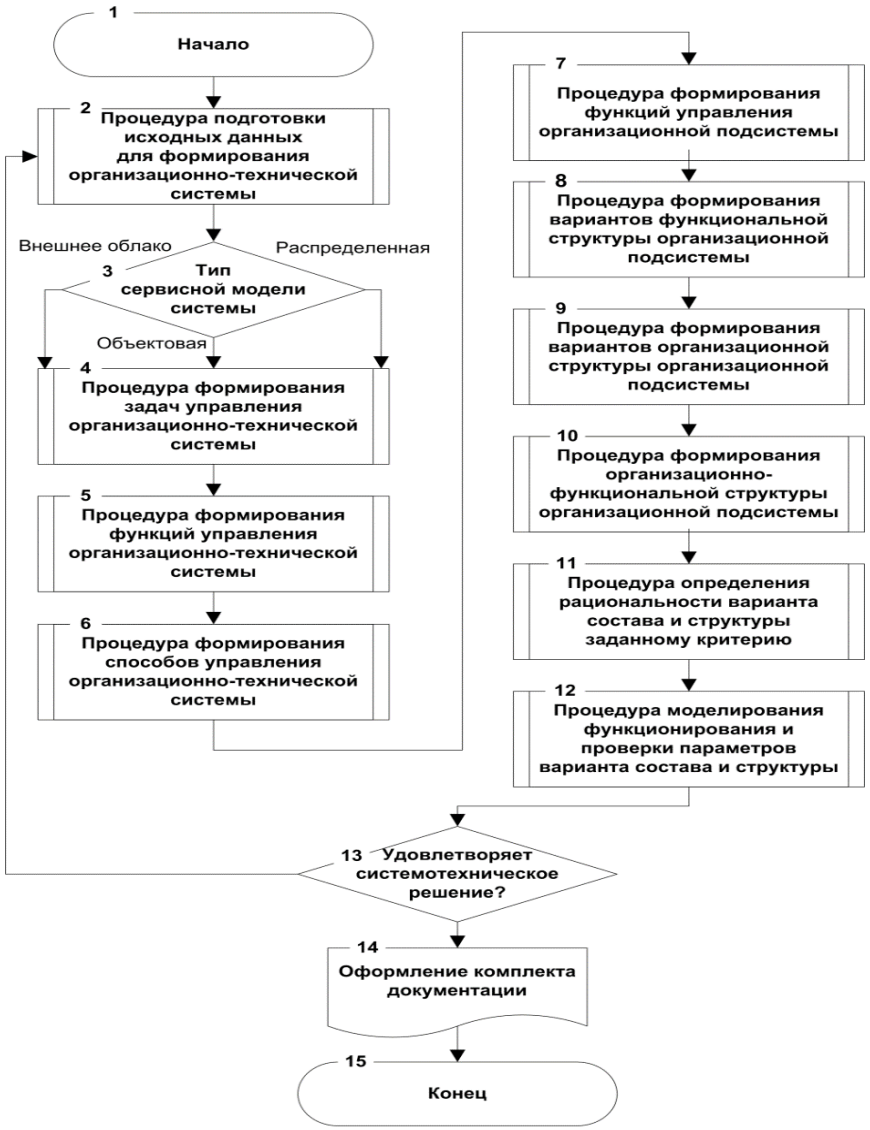

Рисунок 3.7 – Блок-схема комплексной методики синтеза киберполигона

Разработанная комплексная методика синтеза, отличающаяся учетом особенностей нового иерархического организационно-технического компонента специализированных информационных сервисов управления ведомственной СОИБ посредством единства процедур частных методик синтеза его организационной и технической структур, что обусловливает корректность и достоверность результатов управления в организационной системе согласно пространству возможных стратегий.

Частная методика синтеза организационной структуры приведена на рисунке 3.8. Процедуры методики отличаются применением стратифицированной онтологической модели управления в виде онтографа $G^{o}_{КП}$ семплированной формальной модели деятельности телеком-оператора и уровневой архитектуры формирования и предоставления специализированных сервисов в ведомственных СОИБ, обеспечивает адекватность описаний нагрузочных характеристик на компоненты организационной структуры при реализации нескольких сервисов различных треков КП.

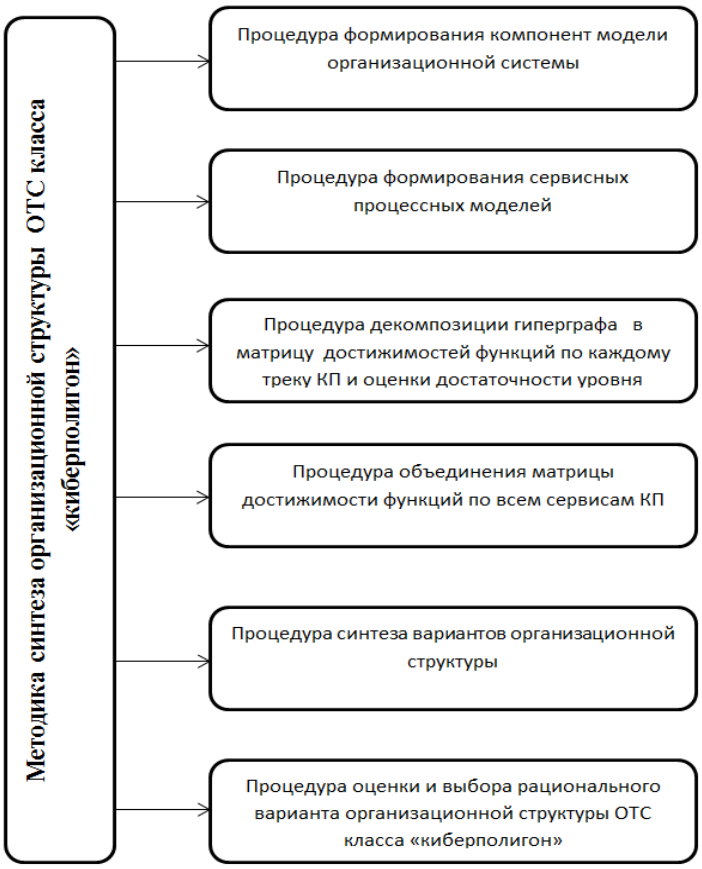

Рисунок 3.8 – Блок-схема методики синтеза организационной структуры киберполигона

Процедура формирования сервисных процессных моделей заключается в формировании ориентированного ациклического (разомкнутого) гипероргафа $G^{c}_{КП}$ в виде ∅ непустого конечного множества сгруппированных элементов $N^{o}_{Тп,КПi}$ из подмножеств вершин $\left\{\{N^{o}_{Тп,ТК,КПi}\}\{N^{o}_{Тп,ТО,КПi}\}\{N^{o}_{Тп,ТИ,КПi}\}\right\}$, индексированных в соответствии с треками КП, и однонаправленных i,j – связей между ними $E^{c}_{КПij}$.

Процедура синтеза вариантов организационной структуры является решением задачи поиска экстремального значения оценочной функции $F\left\{N^{o}_{Тп,КПi}, E^{c}_{КПij}\right\}$ из k-вариантов

$$F(X_{ik}) \rightarrow \max(\min), \tag{3.11}$$

где X_{ik} – вектор параметров вершин;

$I, C_i, R_i, K_i, t_i, D_i, L_i$ – параметры i-вершины (функции, затраты, компетентность, готовность, продолжительность принятия решений, деятельность, территориальность), при ограничениях

$$\{f(X_{ik})\} >< \{X_{jo}\}$$

по критерию готовности для $\forall i = 1, N: \sum_{j=1}^{N} a_{ij}^{r,\dots,m} = 1$,

$$K_r = \sum_i Q_i * \prod_{j=1} Kr_{ij}^{r,\dots,m} \left(a_{ij}^{r,\dots,m}\right) = max, \quad (3.12)$$

при $\sum_{i=1}^{n} Q_i = 1$, $R = \sum_i Q_i (\sum_{j=1}^{N} R_{ij}\, a_{ij}^{r,\dots,m} / \sum_{j=1}^{N} a_{ij}^{r,\dots,m}) \geq R_o$, $\sum_{r,\dots,m} C^{r,\dots,m} < C_o$.

Процедура оценки и выбора рационального варианта организационной структуры ОТС класса «киберполигон» с учетом принятых ограничений и допущений проводится на основе критериев достижимости целей, оперативности (готовности организационных компонент и их взаимодействия), компетентности, внутренних киберрисков, стоимости.

Разработанные процедуры методики синтеза технической структуры и технико-экономического обоснования вариантов построения КП представлены на рисунке 3.9.

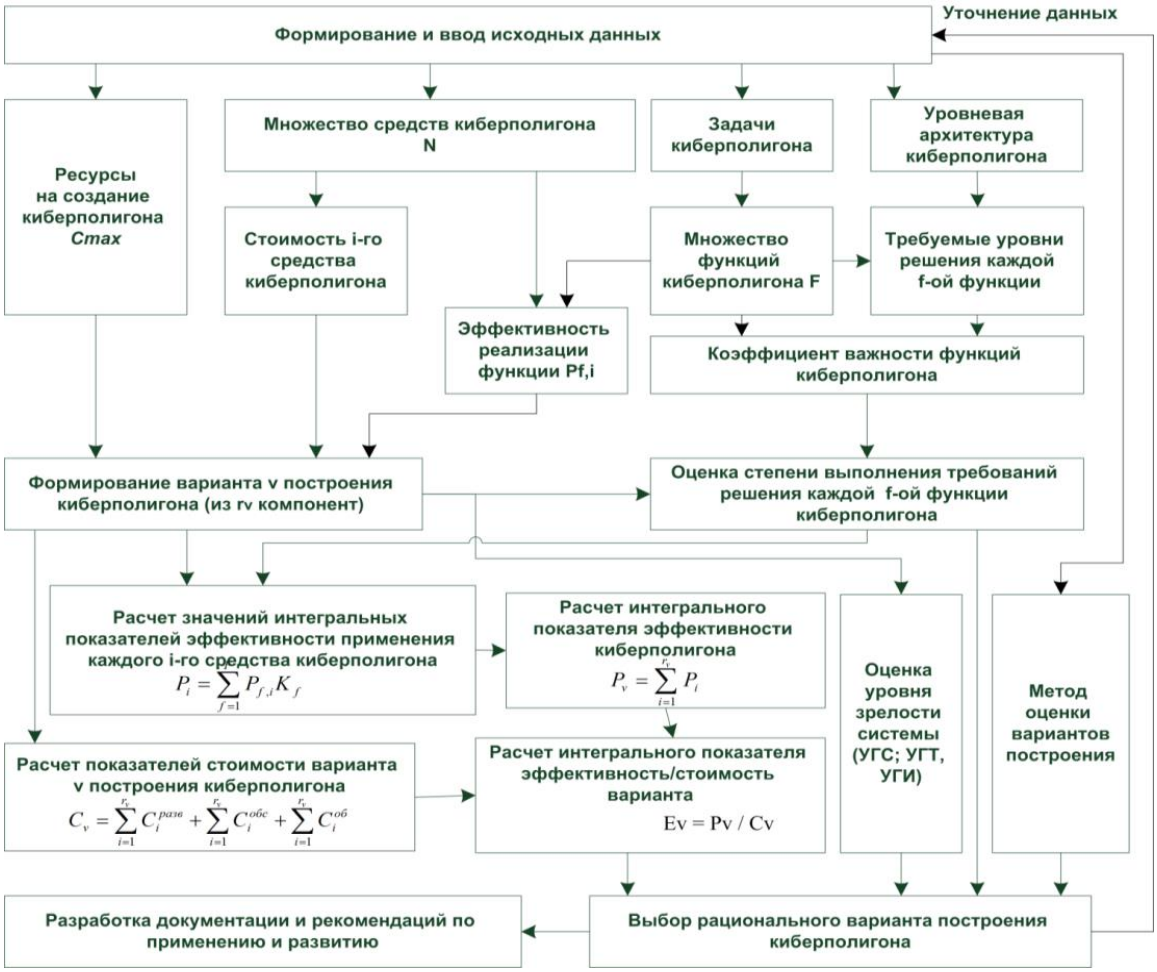

Рисунок 3.9 – Блок-схема методики синтеза технической структуры КП

Сущность предложенной оригинальной методики заключается в том, что в исходные данные процедур оценки, в качестве которых используются технические параметры и стоимостные показатели компонентов, входящих в инфраструктуру КП, дополнительно введены степени решения соответствующих функциональных задач каждым компонентом, а также весовые коэффициенты важности задач. Это позволяет с учетом имеющихся ресурсных ограничений формировать план развития с учетом динамики поэтапного создания и модернизации ОТС класса «киберполигон».

Первоначально процедурами предложенной методики определяется и выбирается конкретный тип средства по каждой частной функциональной задаче, а затем определяется количество и состав используемых средств в инфраструктуре КП в целом. Особенности технологий управления совокупностью разнотипных средств управления ИБ, моделируемой разнородной информационной инфраструктурой, могут отражаться на необходимости применения комплексных решений системотехнического построения средств управления как по отношению к составу используемых средств, так и к протоколам информационно-логического взаимодействия для создания внутренней доверенной среды управления ИБ КП. Возможные решения такого класса зада исследованы и опубликованы учеными университета и соискателями.

Методика технико-экономической оценки вариантов построения КП позволяет ранжировать альтернативные варианты по величине показателя их эффективности для выработки решения и осуществлять сравнительную оценку на основе метода оценки вариантов, заданного в исходных данных методики синтеза.

Для повышения обоснованности выбранного решения реализуется процедура оценки уровня зрелости системы (киберполигона), которая позволит осуществить коррекцию результатов оценки эффективности варианта построения КП не только за счет показателей оценки УГТ уровня готовности технологий (применяемых средств)

$$[\text{УГТ}]_{n\times 1} = \begin{bmatrix} \text{УГТ}_1 \\ \dots \\ \text{УГТ}_n \end{bmatrix}, \tag{3.13}$$

а также уровня готовности интеграции УГИ компонент КП

$$[\text{УГИ}]_{n\times n} = \begin{bmatrix} \text{УГИ}_{11} & \dots & \text{УГИ}_{1n} \\ \dots & \dots & \dots \\ \text{УГИ}_{n1} & \dots & \text{УГИ}_{nn} \end{bmatrix} \tag{3.14}$$

и, соответственно УГС, уровня готовности системы (киберполигона)

$$[\text{УГС}]_{n\times 1} = \begin{bmatrix} \text{УГС}_1 \\ \dots \\ \text{УГС}_n \end{bmatrix} = [\overline{\text{УГИ}}]_{n\times 1} \times [\overline{\text{УГТ}}]_{n\times 1}\,. \tag{3.15}$$

Результаты проведенных расчетов УГС киберполигона показали, что погрешность оценки без учета УГИ составляет более 6 %, и в случае завышенной оценки эффективности варианта построения КП приведет к дополнительным незапланированным затратам при его внедрении и обеспечении эксплуатации в ведомственной СОИБ.

С целью практической отработки вариантов возможной реализации функциональных требований к конфигуратору технологической платформы киберполигона разработан прототип программы для ЭВМ «Модуль-конфигуратор киберполигона» (далее – Модуль), интерфейс которого представлен на рисунке 3.10, а сравнительная оценка его характеристик представлена на рисунке 3.11.

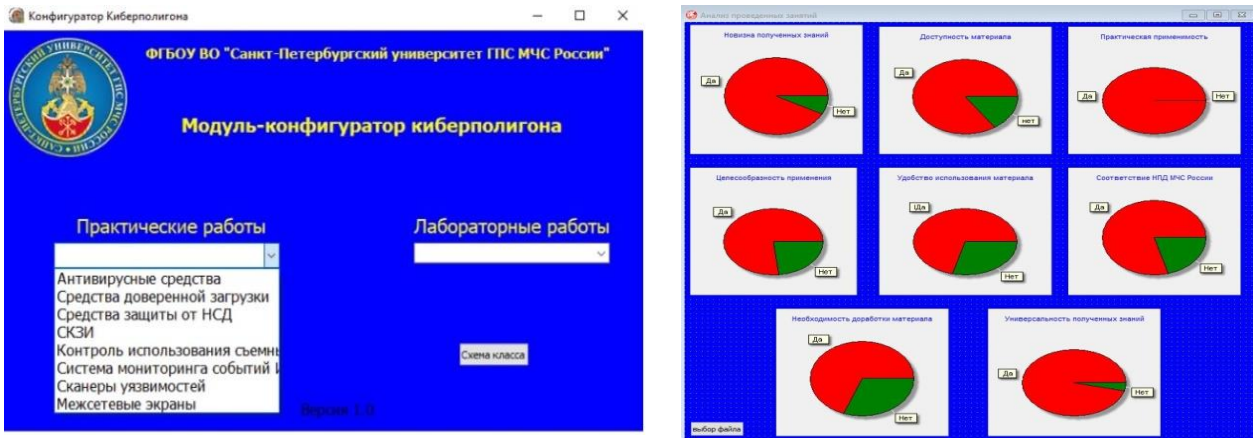

Рисунок 3.10 – Интерфейс «Конфигуратор киберполигона»

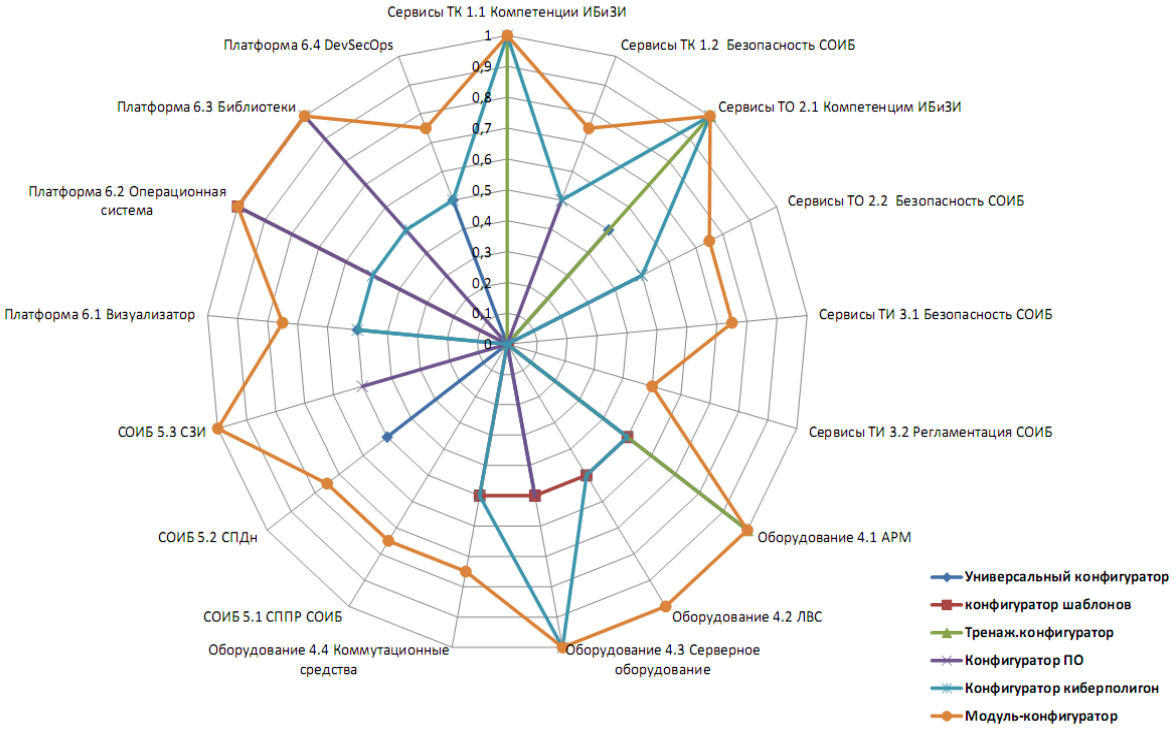

Рисунок 3.11– Оценка технического уровня разработанного конфигуратора киберполигона

Результаты научно-исследовательской работы (НИР) «Поисковые исследования перспективных цифровых технологий непрерывной киберсреды в интересах подготовки, переподготовки и повышения квалификации специалистов по ИБ и защите информации на основе интеграции образовательных и инфраструктурных ресурсов МЧС России» (шифр «Киберсреда») легли в основу создания компонента НОК ИБ (далее – киберполигон МЧС России) и были реализованы на начальных стадиях жизненного цикла киберполигона МЧС России в соответствии с ГОСТ 34.201-2020, ГОСТ 34.602-2020, ГОСТ 34.601-90 (Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания).

Соответствие результатов НИР этапам работ на стадиях 1-3 представлено следующим образом.

Стадия 1 «Формирование требований к АС»

На данной стадии были выполнены все ключевые этапы работ, предусмотренные стандартом, на основании материалов НИР «Киберсреда».

1.1. Обследование объекта и обоснование необходимости создания АС:

В рамках НИР (Раздел 1, Введение) был проведен комплексный анализ исходных данных, включая нормативные правовые акты РФ и МЧС России, а также результаты предшествующих НИР («Вариант», «Модель»). Были выявлены ключевые противоречия и проблемы в существующей системе подготовки специалистов по ИБ, что послужило формальным и содержательным обоснованием необходимости создания киберполигона как компонента НОК ИБ.

1.2. Формирование требований пользователя к АС:

Цели и задачи НИР (Введение, Раздел 2.1) были сформулированы исходя из потребностей МЧС России в повышении уровня профессиональных компетенций должностных лиц. В отчете определена целевая аудитория (специалисты по ИБ), а также сформулированы основные требования к функциональности системы через описание сервисов различных треков (образовательного, испытательного, трека киберучений). Это позволило определить ключевые характеристики будущей системы с точки зрения конечных пользователей.

1.3. Оформление отчета о выполненной работе и заявки на разработку АС

Итоговый отчет о НИР «Киберсреда» является формальным документом, завершающим данный этап. Кроме того, в Приложении Б к отчету был разработан «Проект технического задания на выполнение опытно-конструкторской работы по созданию системы непрерывной образовательной киберсреды...» (шифр «КИБЕРПОЛИГОН-МЧС»), который является прототипом заявки на разработку и основой для следующей стадии.

Стадия 2 «Разработка концепции АС»

Результаты НИР «Киберсреда» полностью покрывают содержание работ на данной стадии.

2.1. Изучение объекта:

На основе данных, полученных на стадии 1, в НИР (Раздел 2) было проведено углубленное изучение объекта автоматизации – процесса непрерывной подготовки специалистов по ИБ в условиях цифровой трансформации МЧС России.

2.2. Проведение необходимых научно-исследовательских работ:

Вся НИР «Киберсреда» по своей сути являлась комплексом поисковых научно-исследовательских работ, направленных на определение перспективных технологий, методологических и технологических подходов к созданию киберполигона.

2.3. Разработка вариантов концепции АС и выбор варианта концепции АС:

В Разделе 2 отчета «Разработка концепции, методологии и технологии построения и функционирования непрерывной образовательной среды...» детально проработана и представлена единая, научно обоснованная концепция киберполигона. Концепция определяет цели, основополагающие принципы, организационную (трехуровневую) и функциональную структуру системы, что является прямым выполнением данного этапа.

2.4. Оформление отчета о выполненной работе:

Раздел 2 и весь отчет о НИР в целом являются итоговыми документами, фиксирующими разработанную концепцию.

Стадия 3 «Техническое задание»

Данная стадия инициирована в рамках НИР «Киберсреда» путем выполнения ключевого этапа.

3.1. Разработка и утверждение технического задания на создание АС:

В рамках НИР «Киберсреда» был разработан проект Технического задания (ТЗ) на выполнение опытно-конструкторской работы. Проект содержит все основные разделы, предусмотренные для ТЗ, включая наименование и цели ОКР, тактико-технические требования к изделию, требования к видам обеспечения, этапы выполнения работ и требования к документации. Проект ТЗ является итоговым документом, формализующим все требования, и предназначен для запуска следующего этапа жизненного цикла – опытно-конструкторской работы.

Таким образом, результаты исследований успешно внедрены в изделие киберполигон МЧС России на его начальных стадиях жизненного цикла: 1 «Формирование требований к АС», 2 «Разработка концепции АС», и создала необходимую основу для стадии, 3 «Техническое задание» в соответствии с ГОСТ 34.601-90. Результаты НИР являются необходимой фундаментальной научно-методической базой для перевода киберполигона МЧС России на следующие стадии жизненного цикла: эскизное и техническое проектирование.

4. Апробация результатов на экспериментальном функциональном фрагменте непрерывной образовательной киберсреды с применением киберполигона

Апробация результатов прикладных научных исследований, полученных в НИР «Киберсреда», была проведена с применением специально развернутого в Санкт-Петербургском университета ГПС МЧС России экспериментального функционального фрагмента непрерывной образовательной киберсреды с применением киберполигона для МЧС России (далее – Фрагмент).

Создать натурный прототип фрагмента НОК, учитывая территориально-распределенный характер, необходимость задействования ведомственного коммуникационного ресурса и другие

организационные и технические сложности, достаточно проблематично в рамках НИР, поэтому в качестве объекта исследований выступает функциональный фрагмент, который должен быть укомплектован как экспериментальный – для отработки задач научных исследований, а не инфраструктурный прототип киберсреды, который должен быть передан в опытную эксплуатацию, а в последующем – в штатную, со всеми вытекающими обстоятельствами.

Так как НОК ИБ будет развертываться с задействованием части ресурсов ведомственной цифровой информационной инфраструктуры, то взаимодействие информационной инфраструктуры «непрерывной образовательной среды» с ведомственной инфраструктурой должен реализовать интегрированный компонент – «ядро интегрированной киберсреды» посредством определенной части коммуникационных средств и средств управления из состава «киберполигона».

«Киберполигон университета», как инфраструктурный проект, планово создается с применением средств защиты информации, переданных различными производителями, а также коммуникационных и информационных средств университета, для обеспечения образовательного процесса, в первую очередь, профессиональной переподготовки и повышения квалификации должностных лиц территориальных органов. Киберполигон университета, как и любой инфраструктурный проект по стадиям реализации, имеет, в настоящее время, определенную реализованную взаимоувязанную часть серверного оборудования, коммуникационного и информационного ресурса со средствами защиты информации, которые используются в учебном процессе и являются соответственно «действующей инфраструктурой киберполигона», т.е. частью «киберполигона университета» определенной стадии его построения.

Замысел построения «киберполигон университета» реализуется в соответствии с наработками, которые были получены в НИР «Вариант» в 2023 году, а также концептуальными положениями, методологических и технологических основ. получившими свое развитие в НИР «Киберсреда» в части построения ведомственного киберполигона в рамках создания НОК ИБ на основе ведомственных образовательных ресурсов и информационной инфраструктуры.

Согласно замыслу, в киберполигоне необходим «конфигуратор киберполигона», как интегрирующий компонент различных функциональных модулей и его инфраструктурных компонент.

Фрагмент предназначен для проверки концептуальных, методологических и технологических основ и положений, выработанных в НИР, для последующего его расширения и развития в ведомственной образовательной и информационной инфраструктуре, в том числе перспективной системы управления и ИБ киберполигона как ядра НОК ИБ.

Функциональный фрагмент сформирован из доступных и бесплатных программных и программно-аппаратных средств в составе и количестве, достаточном для:

- подтверждения возможности организации сервисов ограниченного функционала треков организационно-технической системы класса «киберполигон»;
- подтверждения реализуемости положений концепции «сервис-ориентированных систем» для широкого класса ведомственных задач (от организации и обеспечения проведения киберучений должностных лиц, выполняющих профессиональную деятельность в области информационной безопасности, в масштабе ведомства и образовательного процесса, применительно к потребностям и условиям территориальных органов, до оказания коммерческих услуг в области ИБ: платные услуги дополнительного профессионального образования, аудит ИБ информационных активов пользователей и т.д.).

Архитектура экспериментального функционального фрагмента НОК ИБ с применением киберполигона представлена в виде совокупности организационной, функциональной и технологической схем Фрагмента, в основе которых перечень заданных средств (оборудования).

В киберполигоне применен «конфигуратор киберполигона», как интегрирующий компонент различных функциональных модулей и его инфраструктурных компонент.

Функционально-модульная структура Фрагмента для организации проверок (испытаний) характеристик сервисов треков киберполигона (образовательного, испытательного и киберучений/кибертренировок) при подготовке, профессиональной переподготовке и повышении квалификации кадров скомпонована.

В соответствии с Распоряжением начальником университета разработаны Программа и методики проверок (испытаний) Фрагмента и утверждены. Определены, объект проверок (испытаний), цели проверок (испытаний), состав комиссии, сроки, место и порядок их проведения.

Объектом проверок (испытаний) определен экспериментальный функциональный фрагмент НОК ИБ с применением киберполигона.

Программой проверок (испытаний) Фрагмента определены:

- объект проверок (испытаний),
- его состав и назначение;
- цели и задачи проверок (испытаний),
- объем проверок (испытаний);
- условия, режимы, порядок, место проведения, виды и этапы проверок (испытаний);
- материально-техническое обеспечение проверок (испытаний), обеспечение защиты информации и персональных данных, отчетность;
- 8-мь методик проверок (испытаний).

Проверки (испытания) проводились на территории Санкт-Петербургского университета ГПС МЧС России в соответствии с Программой и методиками проверок (испытаний) Фрагмента. Проверки (испытания) Фрагмента по возможности организации сервисов профориентированного образования по направлению информационной безопасности и организации сервисов формирования, апробации и внедрения новых дидактических средств (методов) проводились в ходе планового образовательного процесса университета: по дисциплине «Информационная безопасность и защита информации» в учебной группе САиУ41.131ГЗ (03.10.2024); по дисциплине «Аттестация объектов информатизации по требованиям безопасности информации» в учебной группе 24.28.452 (09.10.2024), в учебной группе 24.43.452 (23.10.2924); по дисциплине «Введение в специальность» по специальности 10.05.03 «Информационная безопасность автоматизированных систем (уровень специалитета)» в учебной группе ИБ11.210 (19.09.2024), а также на мероприятиях университета по профессиональной ориентации учащихся образовательных организаций общего образования.

Результаты проверок (испытаний) Фрагмента в рамках текущих образовательных процессов подготовки, профессиональной переподготовки и повышения квалификации специалистов по ИБ, показывают ограниченность состава, перечня и количество типовых средств и оборудования для обеспечения возможности организации сервисов образовательного трека, трека киберучений/кибертренировок, испытательного трека организационно-технической системы на базе образовательной организации, а также ее системы управления и ИБ.

Результаты проверок (испытаний) Фрагмента подтвердили корректность и реализуемость концептуальных, методологических и технологических основ и положений, выработанных в ходе прикладных исследований в части:

- функциональности технологических решений по построению и функционированию НОК ИБ, интегрированной с ведомственной информационной инфраструктурой. Подтверждена возможность реализации управления в трехуровневой организационно-технической системе класса «киберполигон», предоставления сервисов трека Фрагментов в интересах пользователей территориально-распределенной системы;
- функциональности технологических решений образовательного трека, трека киберучений/кибертренировок и испытательного трека Фрагмента в рамках текущих образовательных процессов подготовки, переподготовки и повышения квалификации специалистов по ИБ.

Подтверждена возможность организации полного перечня сервисов ограниченной функциональности различных треков текущим составом типовых средств Фрагмента для текущей образовательной деятельности уровня высшего образования (специалитет по направлению подготовки 10.00.00 «Информационная безопасность»), дополнительного профессионального образования (повышения квалификации и профессиональной переподготовки в сфере информационной безопасности и защиты информации), а также профориентации учащихся образовательных организаций общего образования.

- функциональности системы управления и ИБ киберполигона, как ядра НОК ИБ. Подтверждена возможность многоуровневого мониторинга (управления) коммуникационного слоя, информационного слоя и слоя средств защиты информации информационной инфраструктуры Фрагмента и управление конфигурированием средств и ресурсов в зависимости от текущих оперативных и плановых задач, в соответствии с заявками на предоставление (организацию) сервисов треков Фрагмента;
- возможности применения результатов испытаний Фрагмента на этапах создания, ввода в эксплуатацию и обеспечения функционирования перспективной системы управления и ИБ киберполигона как ядра НОК ИБ.

Основные результаты апробации функциональности средств и технологий системы управления и ИБ киберполигона показывают возможность применения их как ядра НОК ИБ.

В ходе апробации испытательного трека (согласно методике №7) была проведена проверка методов обеспечения киберустойчивости пространственных данных (ПД). Под киберустойчивостью понимается способность ПД быть целостными, аутентичными и доступными. Важность именно этих свойств подтверждается экспертными опросами [96].

Для этого была использована имитационная модель распределенной сети, которая показала, что предложенные методы адаптивного управления ресурсами позволяют снизить риск нарушения доступности ПД в условиях деструктивных воздействий до 50%. Полученные результаты подтверждают применимость разработанных подходов в инфраструктуре киберполигона МЧС России.

Целостность и аутентичность ПД достигается путём применения средств криптографической защиты информации (СКЗИ). Практическое применение СКЗИ регулируется соответствующими нормативно-правовыми документами. Отдельного изучения требует вопрос распространения доверия в НОК.

Особенности распространения доверия в НОК

Возможные схемы распространения доверия в НОК включают в себя:

а) схему непосредственного доверия. В основе этой схемы лежит использование самоподписанного сертификата удостоверяющего центра (УЦ), который выступает в роли источника доверия.

Основным преимуществом является простота реализации и независимость от внешних центров доверия, что подходит для небольших групп участников.

Однако основной недостаток заключается в уязвимости при передаче сертификатов через незащищённые каналы. Это может привести к подмене сертификатов злоумышленником и снижению уровня доверия.

Достаточно сложно применимо для НОК, в силу значительного количества разнесённых в пространстве территориальных подразделений МЧС России;

б) схему жёсткого подчинения, которая предполагает выделение одного главного удостоверяющего центра, который контролирует иерархию доверия.

Главный центр подписывает ключи других участников, что создаёт строгое подчинение и централизованное управление.

Основное преимущество состоит в том, что управление системой становится проще и более предсказуемым.

Однако схема обладает серьёзным недостатком – зависимость всей системы от главного центра делает её уязвимой в случае его компрометации или выхода из строя.

Применимо для задач НОК в случае решения вопроса о том, какое подразделение будет Главным УЦ;

в) схему кросс-сертификации, которая применима для установления доверительных отношений между независимыми или условно независимыми организациями, которые хотят сохранить свою автономию.

Суть кросс-сертификации заключается в взаимной выдаче сертификатов, которые обеспечивают доверие между центрами без подчинения одного другому.

Основное достоинство схемы – сохранение суверенитета участников и гибкость. Однако схема становится сложной в управлении при увеличении числа участников, что требует значительных усилий по координации и обновлению сертификатов. Примером такой ситуации может служить Россия в 2015 году, когда в ней существовало более 450 удостоверяющих центров, что делало использование этой схемы трудоёмким и сложным.

Достаточно сложно применимо для задач НОК по причине того, что в МЧС России значительное количество территориальных подразделений;

г) мостовую схему (Bridge CA), в которой используется мостовой центр, который координирует взаимодействие и доверие между всеми участниками. Основное преимущество состоит в том, что мостовой центр не вмешивается в дела участников и только координирует их работу, что делает управление системой гибким и эффективным при большом количестве участников. Недостаток заключается в сложности управления и необходимости поддержания структуры при увеличении числа центров. Однако мостовая схема доказала свою эффективность при построении пространства доверия, как в случаях создания сетей доверия для государственных структур.

Применимо для задач НОК, особенно если возникнет необходимость интеграции с другими ведомствами;

д) схему с третьей доверенной стороной (ТТП), в которой доверие строится через доверенный центр, через который проходят все транзакции. Эта структура позволяет обеспечить высокий уровень безопасности, так как все действия подтверждаются доверенной стороной. Однако основным недостатком является зависимость от доступности центра ТТП. При недоступности центра останавливается вся транзакционная деятельность, что может быть критично в случае трансграничных взаимодействий. Преимущество схемы заключается в возможности использования её для интеграции систем с разными стандартами криптографии, что особенно актуально при международных взаимодействиях.

Применимо для задач НОК, особенно если возникнет необходимость интеграции с другими ведомствами.

Анализ показал, что каждая из рассмотренных схем имеет свои сильные и слабые стороны. Схема непосредственного доверия проста в реализации, но уязвима к подделке сертификатов. Схема жёсткого подчинения обеспечивает простой контроль, но зависит от главного центра. Кросс-сертификация и мостовые схемы подходят для систем с большим числом участников, но требуют серьёзного управления. Схема с ТТП обеспечивает высокий уровень безопасности, но зависит от доступности центра.

Рекомендации для технического проектирования.

Предлагается развивать гибридные схемы, которые объединяют преимущества различных подходов для создания устойчивых и безопасных систем доверия в условиях многопользовательского распределённого режима работы НОК. Особое внимание следует уделить вопросам защиты от атак на промежуточных этапах распространения доверия и разработке методов предотвращения подделки самоподписанных сертификатов.

Конкретный выбор схемы распространения доверия в НОК определяется на этапе технического проектирования.

Описанным выше образом в НОК решаются такие аспекты киберустойчивости ПД как целостность и атентичность. Обеспечение доступности ПД в НОК реализуется за счёт применения технологий децентрализации.

Обеспечение доступности ПД в НОК

Обеспечение доступности ПД в НОК выступает основной задачей, поскольку от её решения, как показано в исследовании [18], зависят остальные аспекты киберусточивости ПД. В исследовании сформулировано и доказано необходимое и достаточное условие обеспечения целостности, конфиденциальности и доступности. Чтобы обеспечить целостность, конфиденциальность и доступность в информационной системе, необходимо и достаточно выделить ресурс для решения штатных задач ИС и только их.

Ограничение 1. Нарушитель целостности, конфиденциальности и доступности для достижения своих целей обязательно использует часть ресурса ИС.

Ограничение 2. Если задачам выделяется требуемый ресурс, они решаются точно и в срок с вероятностью 100%

Построение модели нарушителя доступности ПД в НОК вытекает из более ранних концепций, уже представленных в исследовании [97].

Актуальность задачи обеспечения доступности НОК в условиях деструктивных воздействий (ДВ) ставит проблему ИБ в ранг первостепенных [98].

Нарушение, известное как отказ в обслуживании (Denial of Service, DoS), появляется при превышении НОК запросами пользователей.

Основополагающие подходы к реализации DoS можно свести к трём ключевым направлениям (стратегиям):

- массированная генерация задач;
- подрыв структурной целостности и функций НОК;
- сочетание первых двух способов.

Первая стратегия охватывает генерацию «штормовых» нагрузок, которые перегружают процессорные мощности и ширину каналов связи. Здесь можно упомянуть ICMP flood и DNS/NTP amplification.

Вторая стратегия касается невозобновляемого расхода системных ресурсов, таких как адресное пространство и оперативная память (например, DHCP starvation и IP-фрагментация).

Комбинированное применение этих тактик позволяет злоумышленникам моделировать ситуацию, где предельное напряжение вызывает нарушение стабильности системы, ставя перед экспертами ИБ сложные задачи по разработке контрмер и восстановлению киберустойчивости.

Этот вариант акцентирует внимание на сложной системе взаимодействий в контексте современного анализа и предполагает глубокую аналитическую работу, как принято в академических исследованиях.

Следуя изложенной выше концепции, реализация обеспечения доступности ПД и НОК осуществляется в рамках теории управления.

Основная цель управления, подразумевающая адаптацию к деструктивным воздействиям, заключается в достижении или поддержании определенного уровня эффективности функционирования НОК, что в аналогичных исследованиях прикладных задач описывается на достаточно высоком научном уровне [99, 100].

Показатель эффективности систем, подобных НОК, обычно интерпретируется через предоставление качества обслуживания (Quality of Service, QoS) [97].

В частности, исследование [101] определяет QoS как функцию экспоненциально взвешенной скользящей средней длины очереди и функцию сброса. В протоколе MQTT эта характеристика измеряется вероятностью успешного прохождения пакета между узлами сети.

Следует отметить, что уровень QoS определяет доступность различных ресурсов НОК, включая программные и аппаратные компоненты, согласно модели FIST: вычислительные модули, оперативную память, каналы связи, устройства ввода-вывода [8].

Имитационная модель обеспечения доступности ПД в НОК

В рамках настоящего исследования предпринята попытка формализации функционирования НОК как сети массового обслуживания (Сети).

Предполагается, что Сеть может быть представлена как совокупность систем массового обслуживания типа G/G/1, характеризующихся произвольными законами поступления заявок (задач) и их обслуживания. Обоснованием для подобной интерпретации служит принцип постепенного распространения задач по НОК, сформулированный в работе [102].

При этом постулируется бесконечная длина очереди, а также отсутствие дедлайнов для задач, что гарантирует их выполнение при наличии необходимого ресурса.

Задача исследования заключается в поиске оператора RU, описывающего распределение ресурсов и задач в пространстве-времени в контексте деструктивных воздействий, определенных подразделе 2.3 «Методология управления киберполигоном как непрерывной образовательной средой информационной безопасности и защиты информации на базе операторного управления»).

Критерием достижения целевого свойства системы является равенство числа решенных задач (K) и числа поставленных задач (K*) на заданном интервале функционирования (T*). Данное равенство, в соответствии с разработанной иерархией показателей эффективности, оценивается через вероятность достижения Сетью своей цели деятельности (ВЦД):

$$P = \frac{K}{K^*} = 1.$$

В рамках разработанной модели FIST [103] задачи интерпретируются как совокупность требуемых производительностей: вычислителей (ΩC), каналов связи (ΩL), памяти (ΩSp) и устройств ввода-вывода (ΩTr).

Для упрощения модели, без потери общности, используется обобщенный тип производительности (Ω), измеряемый в условных единицах в секунду [у.е./с].

Внутренние резервы задач НОК, согласно методу решения задач в условиях деструктивных воздействий из работы [103], трансформируются в допустимое изменение производительности пула (ΔΩ).

Следовательно, требуемая задаче производительность находится в интервале [Ω – ΔΩ; Ω + ΔΩ].

Физические элементы, аналогично задачам, представляются через совокупность доступных производительностей: вычислителей (ωC), каналов связи (ωL), памяти (ωSp) и устройств ввода-вывода (ωTr). Также, для упрощения, используется обобщенный тип производительности (ω), измеряемый в у.е./с. Преобразование между различными типами производительности не предусмотрено.

Целью моделирования является оценка эффективности методов адаптивного управления доступностью ресурсов НОК в условиях деструктивных воздействий посредством исследования специфики оператора

$$P = \frac{F(\omega,\Omega)}{|K^*|} = \frac{|K|}{|K^*|} \quad (3.10)$$

Данный подход позволяет анализировать взаимодействие задач и ресурсов в динамически изменяющейся Сети, учитывая вариативность требуемых и доступных производительностей.

В соответствии с моделью синтеза SOFT, целевое свойство Сети – вероятность достижения Сетью собственной цели деятельности (P), расположенное в левой части уравнения, обладает эмерджентным характером, поскольку представлено безразмерной величиной, в отличие от величин в правой части уравнения, выраженных в у.е./с.

Разработанный метод iSOFT позволяет связать через время решения задачи (T) субстанциальные закономерности, определяющие данное эмерджентное свойство:

$$k \in K = \Omega_k T_k \Rightarrow P = \frac{\sum_{i=1}^{|K|} \Omega_i T_i}{\sum_{j=1}^{|K^*|} \Omega_j^* T_j^*} \quad (3.11)$$

Свойство системы Ω, имеющее размерность у.е./с, не рассматривается как эмерджентное относительно физических элементов ω, поскольку обладает той же единицей измерения. Это свойство, интерпретируемое как требуемая производительность Ω, формируется из физических производительностей ω на основании закономерности, верной для параллельного соединения:

$$\Omega \leq \begin{cases} \sum_{i=1}^{N} \omega_i \\ \min\limits_{i=1,N,} \omega_i \end{cases} \quad (3.12)$$

В данном выражении введена дополнительная переменная N, отражающая количество элементов системы в пуле.

Деструктивные воздействия, согласно предложенной модели, проявляются в нарушении структуры и/или функций системы, что выражается в изменении ω от максимального значения до нуля ($0 \geq \omega \geq \omega_{max}$) и в произвольном времени появления и исчезновения доступной физической производительности («времени жизни» узла Сети).

Каждая задача в модели описывается произведением ΩT (производительность пула, умноженная на время), а каждое устройство, формирующее пул, – произведением ωt. Влияние деструктивных воздействий накладывает дополнительные ограничения, обеспечивая возможность решения узлом выделенной задачи:

$$t \geq T, \forall \omega i \in \Omega. \quad (3.13)$$

Искомый оператор RU, реализуемый Сетью, имеет вид:

$$F(\omega, \Omega) = \begin{cases} \Omega \leq \begin{cases} \sum_{i=1}^{N} \omega_i \\ \min\limits_{i=1,N,} \omega_i \end{cases} = \frac{\sum_{i=1}^{|K|} \Omega_i T_i}{\sum_{j=1}^{|K^*|} \Omega_j^* T_j^*} \\ t \geq T, \forall \omega_i \in \Omega \end{cases} \quad (3.14)$$

В контексте развития сетевых технологий, задача определения оператора F, возможно, представляется типовой задачей теории массового обслуживания, допускающей аналитическое решение. В литературе встречаются работы, например [104], моделирующие Сеть как комплекс СМО M/M/2 с учетом надежности элементов и динамики сетевой структуры, включая задержки распространения информации об отказах.

Другой подход, представленный в [105], основан на анализе нестационарных СМО через систему дифференциальных уравнений Колмогорова-Чепмена.

Несмотря на упрощения по сравнению с моделью FIST (D-FIST), авторы отмечают сложность аналитического решения и прибегают к имитационному моделированию. Аналогичные выводы о сложности аналитического подхода к нестационарным СМО представлены в [106].

Однако детальный анализ выявляет ряд особенностей НОК, ставящих под сомнение эффективность аналитического решения найденного оператора. К таким особенностям относятся:

- дифференцированные требования задач к производительности обслуживающих устройств, включая минимально допустимую; в рамках СМО это решается классификацией заявок или адаптацией потока обслуживания к изменчивости производительности устройств и требованиям заявок, что само по себе является нетривиальной задачей;
- целенаправленные агрессивные воздействия (кибератаки и др.), выходящие за рамки вероятностно-статистического описания;
- динамическое присоединение и отключение узлов;
- незавершение задач узлами;
- поступление заявок через произвольные узлы.

Существующие методы учета данных особенностей (классификация заявок и устройств, метод фаз, модели с переменной структурой и т.д.) приводят к частным аналитическим решениям с жесткими ограничениями. Результирующие системы уравнений, как правило, решаются численно для ограниченного числа устройств (20-30), тогда как реальная НОК может содержать сотни и тысячи узлов.

В связи с этим представляется целесообразным решение поставленной задачи путем имитационного моделирования Сети.

Согласно теореме о независимости решаемых задач [10], информационно-управляющими зависимостями между задачами можно пренебречь. Формальная постановка задачи на моделирование представлена далее.

Дано:

– Tmod – время существования сети (в модели MaxModelTime);

– P* – требуемая ВЦД;
– P – текущая ВЦД.

Максимальная доступная производительность узла (ω) – описывает возможности узла предоставить свои ресурсы задаче.

Минимальная производительность, требуемая задачей (Ω) – нижняя оценка производительности узла. Если производительность узла меньше минимальной требуемой, то узел не берёт задачу, даже если он свободен: $\omega \geq \Omega$.

Максимальное время выполнения задачи (T) – время, которое не может быть превышено узлом, если узел взял задачу в работу.

Максимальное время жизни узлов (t) – описывает деградацию Сети, узел исчезает из Сети, если время его пребывания больше максимального. Если он решает задачу, задача считается потерянной.

Максимальное количество поступающих задач в каждый момент времени (K) – характеризует нагрузку Сети в каждый момент времени.

Максимальное количество присоединяющих к Сети узлов в каждый момент времени (N) – описывает прирост ресурсов Сети в каждый момент времени.

Требуется:

Получить такую конфигурацию Сети, для которой текущая ВЦД будет больше или равна требуемой:

$$P \geq P^*. \quad (3.15)$$

Кроме того, для сформированной конфигурации Сети требуется исследование динамики риска нарушения доступности сетевых ресурсов, а также анализ характеристик Сети как системы массового обслуживания, таких как средняя длина очереди и среднее время пребывания задачи в системе.

Имитационная модель составлена и исследована в среде MatLab.

Результаты имитационного моделирования

Конфигурации Сети, демонстрирующие снижение риска нарушения доступности ресурсов на 10%, 20% и 50% в результате применения предложенных методов, иллюстрируются на рисунках 3.25-3.29 соответственно.

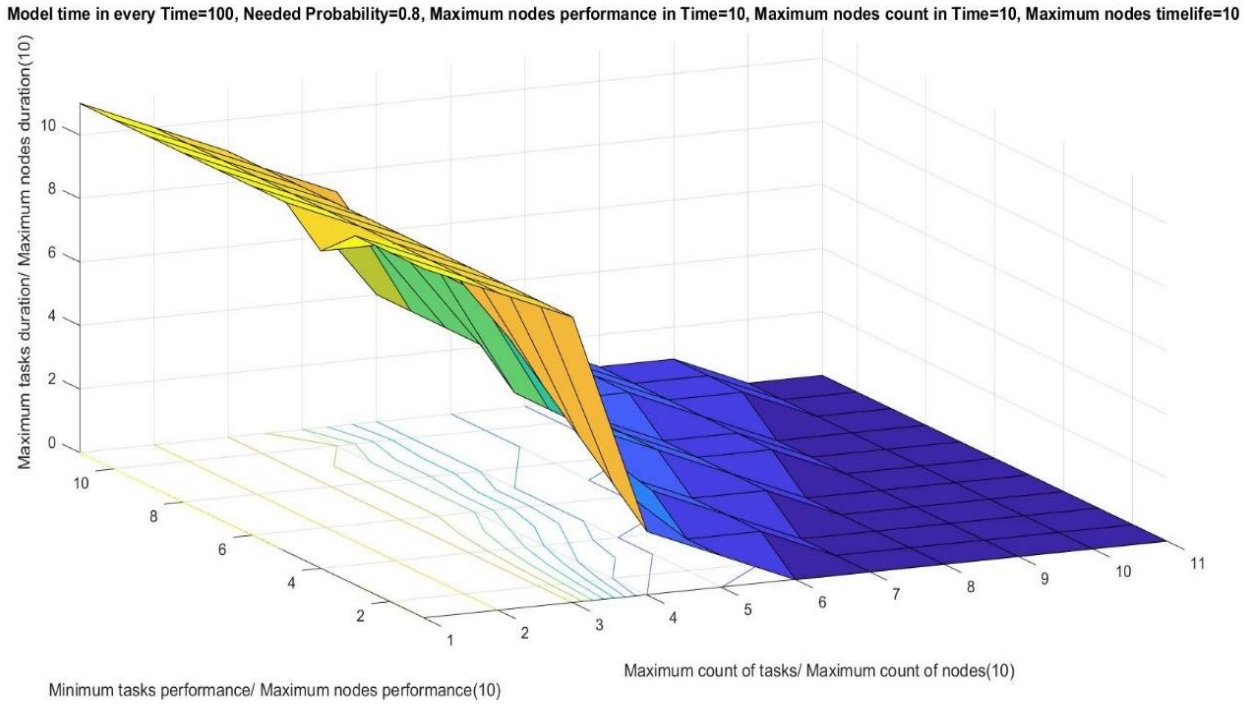

Рисунок 3.25 – Конфигурация Сети, решающей поставленные задачи с вероятностью не ниже 0,8 без применения разработанных методов

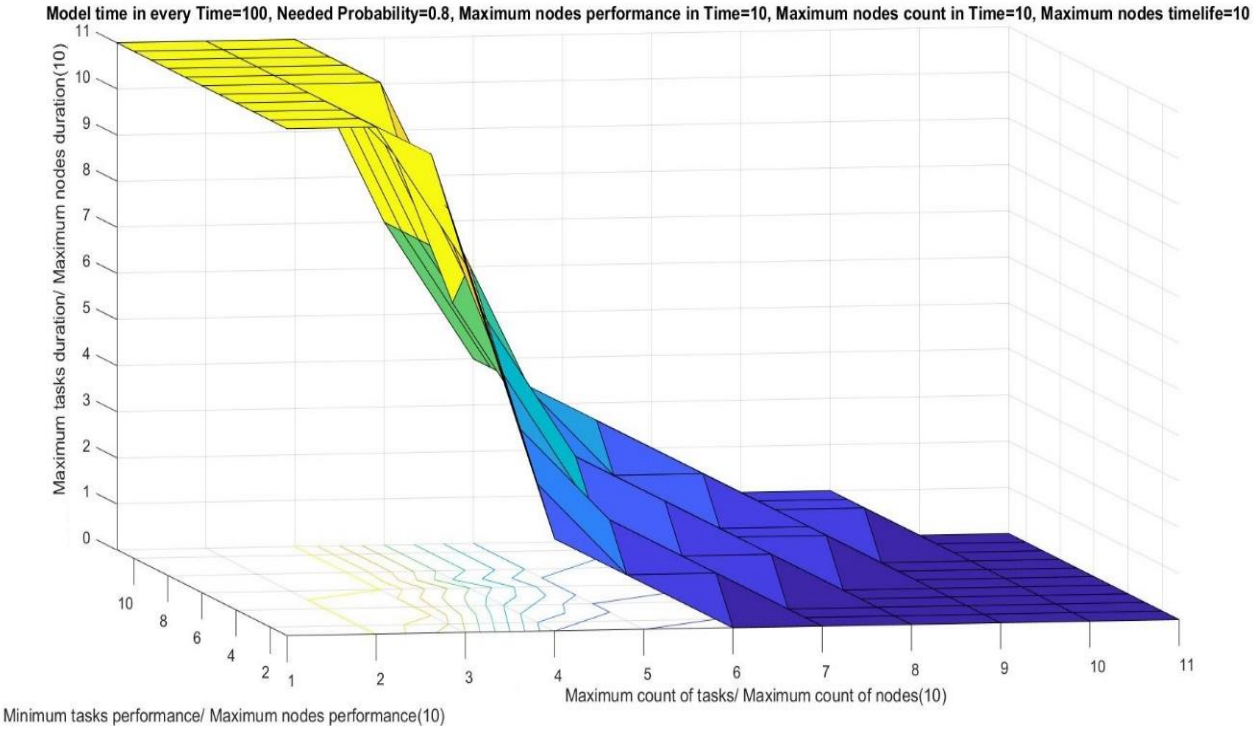

Рисунок 3.26 – Конфигурация Сети, решающей поставленные задачи с вероятностью не ниже 0,8 с применением разработанных методов

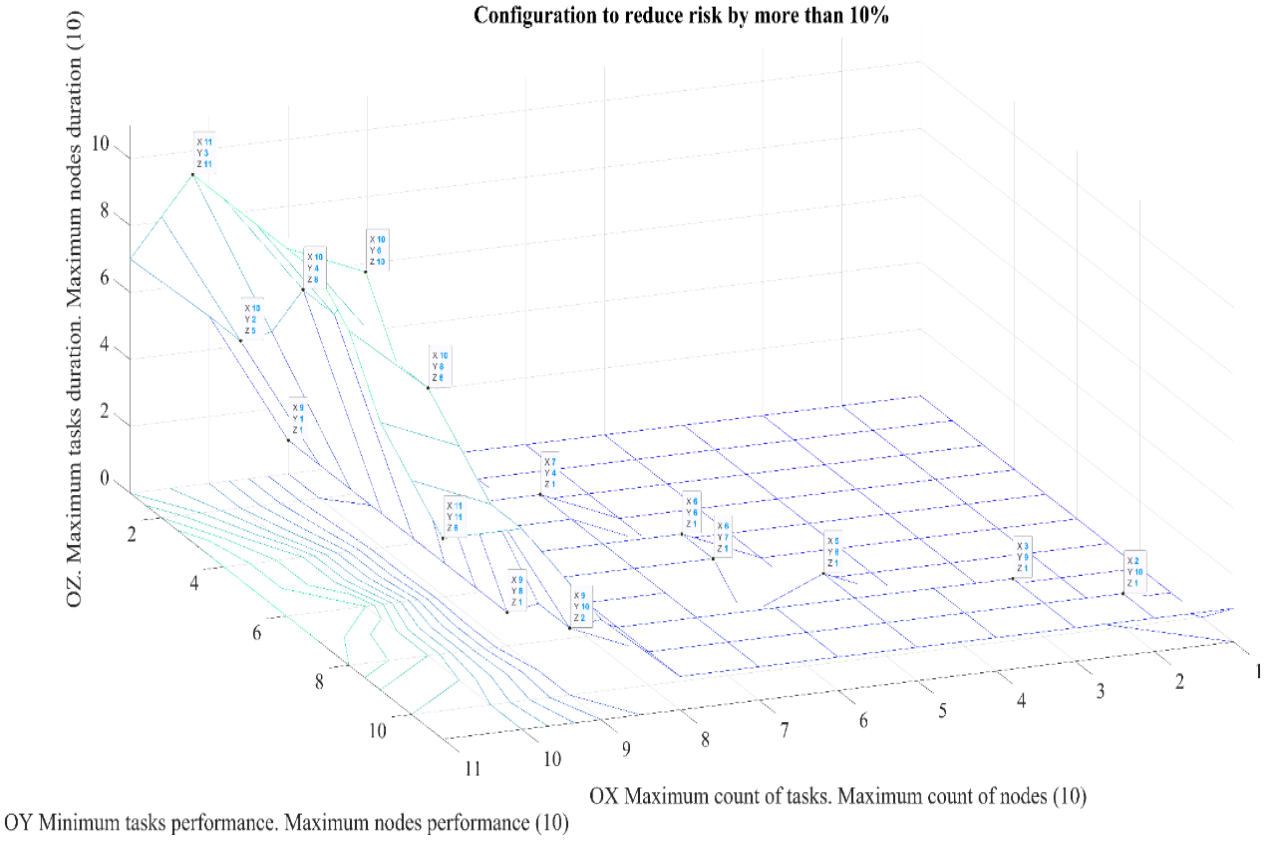

Рисунок 3.27 – Конфигурации Сети, для которых риск нарушения доступности ресурсов снижается в результате применения разработанных методов на 10%

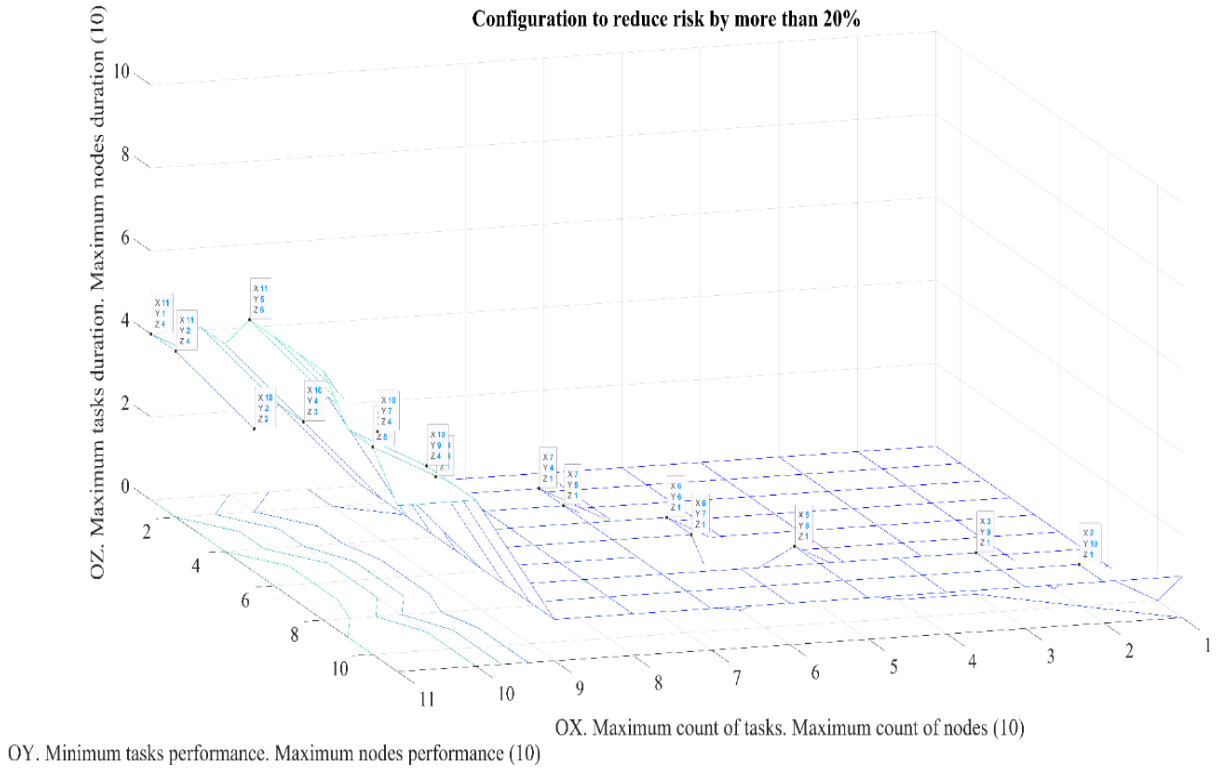

Рисунок 3.28 – Конфигурации Сети, для которых риск нарушения доступности ресурсов снижается в результате применения разработанных методов на 20%

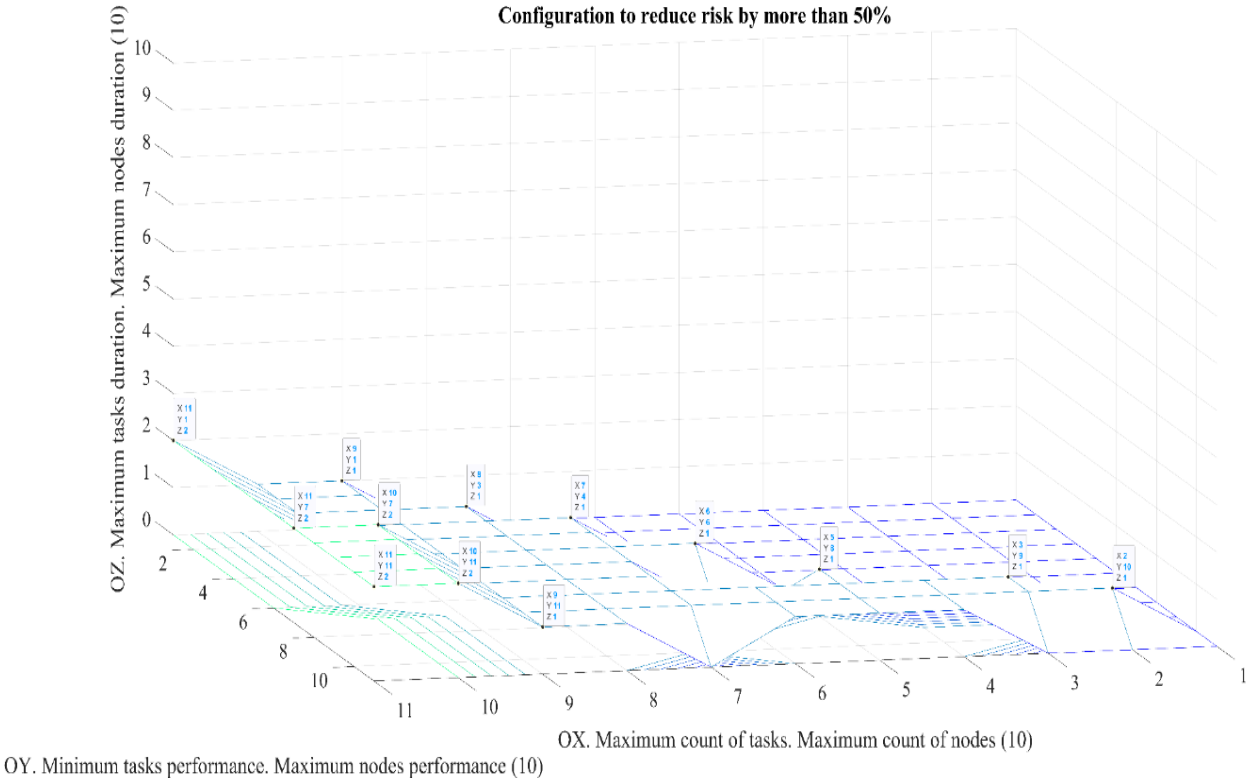

Рисунок 3.29 – Конфигурации Сети, для которых риск нарушения доступности ресурсов снижается в результате применения разработанных методов на 50%

Как видно из рисунков, применение разработанных методов и моделей позволяет сократить риск нарушения доступности ресурсов НОК в условиях деструктивных воздействий до двух раз.

Апробация методов стеганоанализа пространственных данных

Учитывая применительно к стеганографии угроз передачи данных по скрытым каналам [107], наличие и возможности скрытых каналов, которые определены даже нормативно-техническими документами, например, ГОСТ Р 53113.1-2008 [108], образовательный уровень, представленный научно-педагогической школой В.И. Коржика [109], уровень научной проработки различными группами исследователей в области стеганоанализа, например, методического аппарата стеганографического анализа для обеспечения информационной безопасности систем, предложенного специалистами АНО «Институт инженерной физики», АО «ЦНИИмаш» и АО «МПОВТИ» [110], системотехнических решений их реализующих [57], целесообразно в практику защиты пространственных данных киберполигона вводить соответствующие механизмы стеганоанализа, перечень которых систематизирован и представлен в работе [111], и на рисунке 3.30.

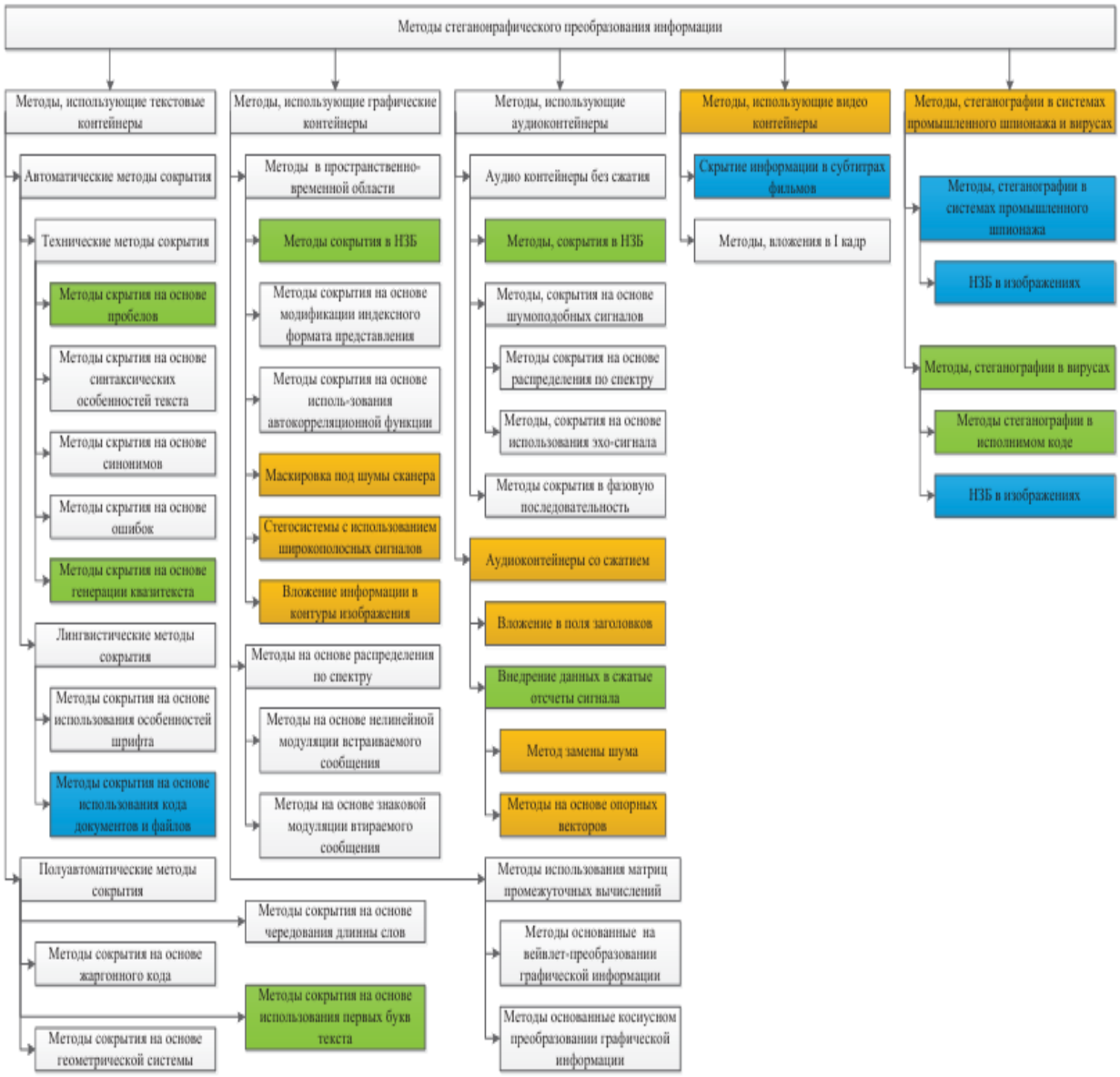

Рисунок 3.30 – Методы стеганографического преобразования информации (источник: [111])

В ходе проверок характеристик испытательного трека экспериментальный функциональный фрагмент непрерывной образовательной киберсреды, сформированной на действующей инфраструктуре киберполигона для МЧС России в рамках текущих образовательных процессов подготовки, профессиональной переподготовки и повышения квалификации

специалистов по информационной безопасности в Санкт-Петербургском университете ГПС МЧС России по Методике №7, была проведена проверка возможности использования типовых программных средств, находящихся в открытом доступе, для решения подобных классов задач, применительно к пространственным данным геоинформационных систем, которые используются в государственной информационной системе РСЧС МЧС России.

Результаты проверки показали, возможность и целесообразность реализации соответствующих компонент в составе киберполигона МЧС России, а соответственно и в цифровой непрерывной образовательной среде информационной безопасности МЧС России.

Таким образом:

1. Положительные результаты проверок (испытаний) экспериментального функционального фрагмента непрерывной образовательной киберсреды с применением киберполигона для МЧС России подтвердили возможность и целесообразность использования такой системы для реализации целей НИР «Киберсреда»:

- подтверждена эффективность концепции сервис-ориентированной системы для киберполигона МЧС России: обеспечивается гибкость, масштабируемость и эффективность использования ресурсов для решения разнообразных задач;
- доказана практическая реализуемость полного перечня сервисов различных треков киберполигона с помощью типовых и доступных средств: система способна решать задачи образовательного трека, трека киберучений/кибертренировок и испытательного трека;
- подтверждена возможность многоуровневого мониторинга (управления) информационной инфраструктурой Фрагмента: система позволяет гибко управлять конфигурацией средств и ресурсов в зависимости от оперативных и плановых задач;
- выявлен достаточный состав программных и программно-аппаратных средств для реализации задач Фрагмента: система базируется на open-source решениях и бесплатных программно-аппаратных средствах, что минимизирует затраты на ее создание.

В целом, испытания подтвердили перспективность разработки полноценного киберполигона для МЧС России как ключевого элемента интегрированной киберсреды ведомства, обеспечивающего высокий уровень кибербезопасности и эффективную подготовку специалистов в этой области.

Результаты испытаний будут использованы для дальнейшего развития киберполигона МЧС России и его интеграции в единую киберсреду ведомства.

2. Киберустойчивость пространственных данных (ПД) в НОК МЧС России является критическим фактором для эффективного функционирования системы. В работе определено понятие киберустойчивости ПД как свойства пространственных данных быть целостными, аутентичными и доступными.

Для обеспечения целостности и аутентичности ПД предлагается использование средств криптографической защиты информации (СКЗИ). Проанализированы различные схемы распространения доверия в НОК, включая непосредственное доверие, жесткое подчинение, кросс-сертификацию, мостовую схему и схему с третьей доверенной стороной. Рекомендовано использование гибридных схем, сочетающих преимущества разных подходов, с учетом специфики МЧС России (большое количество территориально распределенных подразделений). Выбор конкретной схемы должен осуществляться на этапе технического проектирования.

Доступность ПД в НОК обеспечивается применением технологий децентрализации. Разработана имитационная модель НОК как сети массового обслуживания (Сети) типа G/G/1 для анализа доступности ПД в условиях деструктивных воздействий (DoS-атак). Модель учитывает такие факторы, как вариативность производительности узлов, динамическое изменение структуры сети, целенаправленные атаки и другие.

Имитационное моделирование показало эффективность предложенных методов повышения доступности ПД. Результаты моделирования демонстрируют снижение риска нарушения доступности ресурсов НОК до двух раз при применении разработанных методов.

Обеспечение киберустойчивости информационных ресурсов на основе пространственных данных при их актуализации в интегрированной непрерывной образовательной киберсреде должно обеспечиваться комплексом мероприятий по предотвращению инцидентов.

Результаты апробации мероприятий по предотвращению инцидентов на пространственных данных на базе киберполигона показали возможность определения и применения общих механизмов для последующего их использования в практике информационной инфраструктуры МЧС России.

Дальнейшие исследования должны быть направлены на:

- разработку конкретных гибридных схем распространения доверия, адаптированных к структуре МЧС России;
- уточнение и развитие имитационной модели с учетом специфических особенностей функционирования НОК;
- разработку практических рекомендаций по настройке и управлению НОК для обеспечения требуемой киберустойчивости ПД;
- анализ и разработка методов противодействия DoS-атакам, направленным на нарушение доступности ПД.

3. Необходимо разработать механизмы учета территориально-распределенного характера системы, обеспечения информационной безопасности и защиты персональных данных.

Требуется провести дополнительные исследования для оптимизации архитектуры киберполигона и повышения его эффективности и устойчивости к кибератакам.

Заключение

Создание НОК ИБ жизненно важно для повышения квалификации специалистов МЧС России в условиях растущего числа кибератак и угроз информационной безопасности.

В соответствии с предложенной концепцией образовательная среда строится на трёх уровнях: верхний: органы управления; средний: образовательные организации и заинтересованные подразделения; нижний: исполнители образовательных сервисов.

Функционально НОК ИБ поддерживает обучение, повышение квалификации и переподготовку специалистов по информационной безопасности, предоставляя необходимые учебные ресурсы и технологии. Ведомственная НОК ИБ тесно связана с цифровой инфраструктурой МЧС России, что позволяет оперативно получать актуальную информацию и применять полученные знания на практике.

Применение треков киберполигона при реализации методологии и технологий построения и функционирования непрерывной образовательной среды информационной безопасности расширяет его эффективное использование по различным направлениям.

Образовательный трек создает уникальную возможность для курсантов (студентов) и специалистов приобрести практические навыки и компетенции в области информационной безопасности; обеспечивает применение интерактивных компьютерных лабораторий, симуляции атак и защитных сценариев, что позволяет изучать защиту информации в реалистичных условиях; помогает подготовиться к решению нестандартных и высокоприоритетных задач в условиях реальных угроз информационной безопасности.

Испытательный трек ориентирован на проверку эффективности новых инструментов и технологий защиты информации; обеспечивает возможность проведения регулярного тестирования защитных механизмов и выявления слабых мест в системе безопасности; способствует ускоренному внедрению новых эффективных методов защиты и снижению вероятности успешных атак.

Трек кибертренировок и киберучений обеспечивает проведение групповых тренировочных мероприятий, имитирующих реальную обстановку информационного противоборства; повышает способности специалистов быстро реагировать на возникающие угрозы и минимизировать последствия атак; формирует умение действовать командой, укрепляет координацию и улучшает принятие решений в кризисных ситуациях.

В соответствии с организационными подходами интеграция сил эксплуатации НОК ИБ с ведомственной и объектовой системой обеспечения информационной безопасности (СОИБ) обеспечивает условия объединения усилий ведомств и образовательных учреждений по созданию единой системы подготовки и переподготовки специалистов по информационной безопасности, повышая общий уровень профессионализма и совместимости среди сотрудников МЧС России.

Использование информационных ресурсов и технологий в рамках реализации концепции НОК ИБ позволяет собирать и обрабатывать большие объемы данных, необходимых для обучения и анализа угроз. Благодаря тесной интеграции специалисты получают быстрый доступ к актуальной информации и необходимым инструментам для быстрого реагирования на любые события.

Ведущие эксперты регулярно участвуют в разработке учебных программ и тренингов, что повышает профессиональный уровень действующих сотрудников. Постоянное обновление знаний и навыков снижает риски возникновения инцидентов благодаря своевременному реагированию на угрозы.

Координация усилий между ведомственными органами и образовательными учреждениями создает эффективные механизмы раннего предупреждения и устранения угроз. Совместная работа и постоянный мониторинг способствуют быстрой идентификации и устранению возникающих угроз информационной безопасности.

Система управления и безопасности на базе технических решений киберполигона в НОК БИ обеспечивает следующие механизмы безопасности: регулярного контроля и периодической проверки готовности образовательных ресурсов и технологий к обеспечению информационной безопасности; мониторинга активности пользователей, контроля поведения пользователей внутри образовательной среды для предотвращения несанкционированных действий, соблюдения стандартов информационной безопасности, резервирования и восстановления данных (наличия резервных копий и планов восстановления в случае непредвиденных обстоятельств).

Создание и внедрение НОК ИБ, оснащенной треками киберполигона, значительно повышают профессионализм специалистов по информационной безопасности. Интеграция с ведомственной системой СОИБ усиливает возможности реагирования на угрозы и сокращает потенциальные риски нарушений информационной безопасности. Эти меры помогают МЧС России оставаться на переднем крае борьбы с современными киберугрозами и эффективно защищать важные государственные объекты и инфраструктуру.

Список литературы

1. Матвеев А.В., Метельков А.Н., Шестаков А.В. Риски кибератак: ликвидация последствий проявления кибертерроризма и чрезвычайных ситуаций // Вестник Воронежского института ФСИН России. 2023. № 1. С. 98-106.

2. Максимова Е.А., Буйневич М.В., Шестаков А.В. Проактивное управление информационной безопасностью субъектов критической информационной инфраструктуры как сложных организационных систем с динамически меняющейся структурой // Вестник Воронежского института МВД России. 2023. № 2. С. 49-59.

3. Шестаков А.В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. – СПб.: ГУАП, 2016.- 325 с. ISBN: 978-5-8088-1145-4.

4. Метельков А.Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. 2022. № 1. С. 51–60.

5. Метельков А.Н., Шестаков А.В. Киберполигоны и испытательные полигоны: зарубежный опыт защиты информации и систем от киберугроз // 12th International conference on advanced Infotelecommunications (ICAIT 2023). XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании». 28 февраля – 1 марта 2023 года. Т.1. 2023. СПб: СПбГУТ, 2023.

6. Шестаков А.В. Построение киберполигона МЧС России на площадке Санкт-Петербургского университета ГПС МЧС России // I Международный научно-практический форум «Право цифровой

безопасности». Стратегическая сессия – практикум «Цифровая защита от чрезвычайных ситуаций». Программа. 24-25 апреля 2024. Москва. URL: https://mgimo.ru/upload/2024/04/2024-04_digital-law-forum.pdf

7. Шестаков А.В. и др. Цифровая трансформация ведомственных вузов: гармонизация нормативной правовой базы информационной безопасности // Право. Безопасность. Чрезвычайные ситуации. 2024. № 10 (71). С. 70–79. DOI: 10.61260/2074-1626-2024-10-70-79.

8. Грызунов В.В., Шестаков А.В., Брюханов В.А. Выявление проблем информационной безопасности методом систематического обзора литературы // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2024. № 1. С. 104-122.

9. Буйневич М.В., Власов Д.С., Моисеенко Г.Ю. Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024. № 3 (61). С. 2-13.

10. Грызунов В.В. Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 101-115. DOI: 10.31854/1813-324X-2022-8-3-101-116.

11. Грызунов В.В. Метод динамического формирования пулов в информационно-вычислительных системах военного назначения // Информационно-управляющие системы. 2015. № 1(74). С. 13-20. DOI 10.15217/issn1684-8853.2015.1.13

12. Грызунов В.В. Модель геоинформационной системы FIST, использующей туманные вычисления в условиях дестабилизации //Вестник Дагестанского государственного технического университета. Технические науки. 2021. Т. 48. №. 1. С. 76-89. DOI: 10.21822/2073-6185-2021-48-1-76-89.

13. Shestakov A.V., Nesterov A.A. Spatial Data Of Smart Cities: Trust // В сборнике: Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities. Includes selected Papers from International Conference on Advanced Computing & Next-Generation Communication (ICACNGC 2022). Ghent, Belgium, 2024. С. 209-217.

14. Шестаков А.В., Израилов К.Е., Мишин В.Е. Обзор атак на искусственный интеллект: мониторинг информационной безопасности больших данных // В сборнике: Пожарная безопасность: современные вызовы. Проблемы и пути решения. Материалы Всероссийской научно-практической конференции. СПб, 2024. С. 22-28.

15. Шестаков А.В., Тукмачева М.А., Папырина Е.В. Регламентация искусственного интеллекта, больших данных и информационной безопасности для прикладных задач МЧС России // В сборнике: Пожарная безопасность: современные вызовы. Проблемы и пути решения. Материалы Всероссийской научно-практической конференции. Санкт-Петербург, 2024. С. 8-13.

16. Буйневич М.В., Коржик В.И., Яковлев В.А., Изотов Б.В., Старостин В.С. Прогресс в теории прикладной криптографии обзор и некоторые новые результаты. Часть 1. Ключевая криптография // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 126-141.

17. Буйневич М.В., Матвеев А.В., Шестаков А.В. Проблемы применения IT и VR-технологий в области комплексной безопасности // В сборнике: Проблемы и перспективы развития IT- и VR-технологий в области комплексной безопасности. материалы II Всероссийской научно-практической конференции. Екатеринбург, 2023. С. 21-26.

18. Громова Н.Н., Шестаков А.В. Проблематика динамического доступа к цифровым образовательным ресурсам //В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей XII Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.И. Макаренко, сост. В.С. Елагин, Е.А. Аникевич. Санкт-Петербург, 2023. С. 569-575.

19. Шестаков А.В., Тукмачева М.А., Линник В.А. Безопасность жизнедеятельности: информационная безопасность. Схемы и QR-ссылки: учебное пособие. СПб: Типография Любавич, 2023. 108с. ISBN: 978-5-907737-58-7.

20. Коцюба И.Ю., Шестаков А.В. Методы и средства обучения специалистов в области информационной безопасности баз данных // Автоматизация в промышленности. 2023. № 11. С. 61-64.

21. Коцюба И.Ю., Шестаков А.В. Формирование оценочных средств компетентностных моделей в области информационной безопасности // Прикладная математика и вопросы управления. 2023. № 4. С. 107-125.

22. Шестаков А.В., Коцюба И.Ю. Методы и средства формирования и оценки компетенций специалистов в области информационной безопасности на основе многофункционального программно-аппаратного комплекса // Инженерный вестник Дона. 2023. № 12 (108). С. 88-99.

23. Буйневич М.В., Вострых А.В. Программа синтеза семантической структуры учебной дисциплины // Свидетельство о регистрации программы для ЭВМ №2023682552 / Правообладатель СПб университет ГПС МЧС России. Дата публик. 26.10.2023 Бюл.№11.

24. Воронцова А.А., Матвеев А.В. Система управления электронным каталогом терминов по информационной безопасности // Свидетельство о регистрации программы для ЭВМ №2024667433/ Правообладатель СПб университет ГПС МЧС России. Дата публ. 24.07.2024 Бюл. №8.

25. Коцюба И.Ю., Шестаков А.В. Автоматизация корпоративной кадровой политики: компетентностные модели в области информационной безопасности // Автоматизация в промышленности. 2023. № 9. С. 61-64.

26. Шестаков А.В., Линник В.А. Комплексная методика оценки дефицита компетенций в ведомственных системах обеспечения информационной безопасности // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2024. № 10 (78). С. 25–30.

27. Линник В.А., Шестаков А.В. Определение уровня компетенции специалистов в области информационной безопасности // Свидетельство о регистрации программы для ЭВМ №2024683912/ Правообладатель Линник В.А. Дата публикации 14.10.2024 Бюл. №10.

28. Коцюба И.Ю., Шестаков А.В. Механизмы актуализации трудовых функций должностных лиц в области информационной безопасности МЧС России // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2023. № 3. С. 75-83.

29. Синещук М.Ю., Гавкалюк Б.В., Шестаков А.В., Синещук Ю.И. Конфигуратор Киберполигона / Свидетельство о регистрации программы для ЭВМ № 2024619031/ Правообладатель: СПб университет ГПС МЧС России. Опубл. 18.04.2024.

30. Синещук М.Ю., Данилова В.А., Кузнецова К.А. Инфологическая модель организационной системы // В сборнике: Моделирование энергоинформационных процессов. Сборник статей XII национальная научно-практическая конференция с международным участием. Воронеж, 2024. С. 120-123.

31. Синещук М.Ю. Инфологическая модель организационных систем класса «киберполигон» // Вестник Воронежского института ФСИН России. 2023. № 3. С. 140–147.

32. Синещук М.Ю., Гавкалюк Б.В., Шестаков А.В. Комплексная методика и алгоритмы синтеза и оценки рациональности вариантов построения архитектур ведомственных организационно-технических систем класса «киберполигон» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). сборник научных статей. XII Международной научно-технической и научно-методической конференции. в 4-х т., СПб, 2023. С. 322–327.

33. Синещук М.Ю. Синтез корпоративной системы повышения уровня осведомленности персонала в области информационной безопасности // Сибирский пожарно-спасательный вестник. 2024. Т. 32. № 1. С. 88-96.

34. Синещук М.Ю. Выбор оптимального состава средств системы защиты информации предприятия (организации, учреждения) с учетом финансовых ограничений. / М. Ю. Синещук, Ю. И. Синещук // материалы XV Международной научно-практической конференции «Государство и бизнес. Направления социально-экономического развития»: Санкт-Петербург, 2023 г. В 2 т. Т. 1. СПб: ИПЦ СЗИУ РАНХиГС, 2023. с.40–48.

35. Синещук М.Ю., Гавкалюк Б.В., Шестаков А.В. Инфологическая модель и критерии качества решений по построению ведомственных организационно-технических систем класса «киберполигон» // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2023. № 1. С. 121–137.

36. Синещук М.Ю., Гавкалюк Б.В., Матвеев А.В., Шестаков А.В. Методика технико-экономической оценки вариантов построения организационно-технической системы класса «киберполигон» // Инженерный вестник Дона. 2023. № 6 (102). С. 187–200.

37. Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации» от 01.12.2016 №642.

38. Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации» от 28.02.2024 №145.

39. Федеральный закон «О науке и государственной научно-технической политике» от 23.08.1996 №127-ФЗ (ред. от 08.08.2024).

40. Карпенко А.С., Павлова С.М. Цифровая образовательная среда в России: проблемы, опыт внедрения и перспективы // Человеческий капитал, Том 2, №11 (156), 2021. С. 43-52. DOI: 10.25629/HC.2021.12.40.

41. Лейфа А.В., Бодруг Н.С. Методология и технология педагогического проектирования переподготовки инженеров в цифровой образовательной среде вуза. М.: Амурский государственный университет, 2024. 152 с. DOI: 10.22250/9785934934201.

42. Гриншкун В.В., Краснова Г.А. Современная цифровая образовательная среда: ресурсы, средства, сервисы. М.: ООО «Проспект», 2023. 216 с.

43. Меньшина А.С. Развитие моделей смешанного и дистанционного обучения в цифровой образовательной среде профессиональной организации // В сб. Профессиональное образование: методология, технологии, практика. Т.16 Челябинск: Издательство ЗАО «Библиотека А. Миллера», 2023. С132-135.

44. Каледина А.М. Цифровые технологии в образовательной среде // в XIX межвузовском сборнике научных трудов «Актуальные проблемы развития общего и высшего образования». Челябинск: Издательство ООО «Край Ра», 2024. С. 64-69.

45. Гречихина Е.А. Ресурсы цифровой образовательной среды в процессе обучения иностранному языку: классификация, принципы и критерии отбора // В сб. Научный старт-2023 Том часть 1. Институт иностранных языков МГПУ. М.: ООО «Языки Народов Мира», 2023. С.134-137.

46. Бондаренко В.В., Таишева К.С., Пензина Д.П, Теоретические и методические основы формирования цифровой образовательной среды как элемента инновационной системы управления высшим образованием в Российской Федерации // В коллективной монографии «Стратегии повышения конкурентоспособности международной деятельности вузов в глобальном цифровом образовательном пространстве». Пенза: Пензенский государственный аграрный университет, 2023. С. 35-45.

47. ГОСТ Р 59871-2021 Информационно-коммуникационные технологии в образовании. Цифровая научно-образовательная среда. Общие положения.

48. Коблов С.В. Особенности Российской специфики управления ресурсным потенциалом научных и наукоемких организаций на современном этапе экономического развития. М.: ООО «Издательство «Юнити-Диана», 2024. 151 с.

49. Казаренкова Т.Б. Социокультурные и социально-управленческие основы формирования инновационной научно-образовательной среды вуза в условиях развития цифрового общества // Сб. научных трудов «Социокультурные проблемы современного высшего образования. М. РУДН, 2019. С.14-21.

50. Краковецкая И.В. Обеспечение устойчивой конкурентоспособности университетов в цифровой научно-образовательной среде. Дисс. на соиск. уч. степ. д.эк.н. по специальности 08.00.05. Новосибирск: ФГБОУВО «НИНХ», 2021. 635 с.

51. 51 Тарасова А.Н. Трансформация модели академического предпринимательства в системе цифровой экономики. Дисс. на соиск. уч. степ. к.эк.н. по специальности 08.00.01. Йошкар-Ола: ФГБОУ ВО «Поволжский государственный технологический университет», 2022. 176 с.

52. Королев В.И., Гаврилов В.Е. Информационные системы цифровой экономики и подходы к обеспечению их информационной безопасности // Системы высокой доступности. 2019. Т.15. №1. С.38-46. DOI: 10.18127/j20729472-201901-05.

53. Цели развития тысячелетия: доклад за 205 год. Нью-Йорк: ООН, 2015. 75 с. [Электронный ресурс] https://www.un.org/ru/millenniumgoals/mdgreport2015.pdf

54. Нестеров А.Г. Европейские концепции непрерывного образования в начале XXI века // Научный диалог. 2012. Вып. № 5. С.29-38.

55. Постановление ЦК КПСС, Совмина СССР, ВЦСПС «О совершенствовании организации заработной платы и введении новых тарифных ставок и должностных окладов работников производственных отраслей народного хозяйства» от 17.09.1986 №1115 (ред. от 01.07.1991).

56. Закон РФ «Об образовании» от 10.07.1992 № 3266-1.

57. Тертышный Р.С. Разработка и оптимизация информационной системы, предназначенной для выявления и анализа стеганографческих сообщений // Научно-исследовательский центр «Technical Innovations». 2023. № 20. С. 26-31.

58. Постановление Правительства Российской Федерации «О Федеральной целевой программе содействия занятости населения РФ на 1996-1997 годы» от 08.05.1996 №570.

59. Постановление Правительства Российской Федерации «Об осуществлении мониторинга системы образования» от 05.09.2013 № 662.

60. Постановление Правительства Российской Федерации «О мерах государственной поддержки организаций, осуществляющих образовательную деятельность, в рамках федерального проекта «Новые возможности для каждого» национального проекта «Образование» и признании утратившим силу

постановления Правительства Российской Федерации от 29 апреля 2019 г. № 525» от 29 октября 2020 г. № 1759.

61. Распоряжение МЧС России «Об утверждении Ведомственной программы цифровой трансформации МЧС России на 2022 год и на плановый период 2023 и 2024 годов» от 25.07.2022 № 800.

62. ГОСТ Р ИСО/МЭК 27000 – серия стандартов в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности

63. Нормативные правовые акты в сфере информационной безопасности и цифровой экономики. Итоги 2021-2023 г.г. / Аналитический отчет. – М.: Экспертно-аналитический центр InfoWatch, 2024 35 с.

64. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по автоматизации информационно-аналитической деятельности» от 20.07.2022 № 425н (зарегистрирован 22.08.2022 № 69718).

65. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по технической защите информации» от 09.08.2022 №474н (зарегистрирован 09.09.2022 № 70015).

66. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» от 14.09.2022 №533н (зарегистрирован 14.10.2022 № 70515).

67. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» от 14.09.2022 №525н (зарегистрирован 14.10.2022 №70543).

68. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях» от 14.09.2022 №536н (зарегистрирован 18.10.2022 № 70596).

69. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере» от 28.11.2022 №739н (зарегистрирован 22.12.2022 № 71784).

70. Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Специалист по информационным системам» от 13.07.2023 №586н (зарегистрирован 16.08.2023 № 74817).

71. ГОСТ Р 57193-2016 Системная и программная инженерия. Процессы жизненного цикла систем.

72. ГОСТ Р 59330-2021 Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы.

73. Отчет о НИР «Выбор и обоснование рационального варианта построения киберполигона для МЧС России», шифр «Вариант» // Шестаков А.В., Буйневич М.В., Метельков А.Н., Евсеева О.Е., Воронцова А.А., Титова Е.А., Папырина Е.В., Уткин О.В., Синещук М.Ю., Шаталов С.Э., Матвеев А.В., Корольков А.П., Погребов С.А. // Отчет о НИР (итоговый). Номер государственной регистрации: 223111300011-3. СПб: СПб УГПС МЧС России, 2023. 408с.

74. Ukwandu E. et al. A review of cyber-ranges and test-beds: Current and future trends // Sensors. 2020. V. 20(24). №. 24. P. 7148. DOI:10.3390/s20247148.

75. Grimaldi A. et al. Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms / In book: Computer Security. ESORICS 2023 International Workshops. Pp.271-290. DOI:10.1007/978-3-031-54129-2_16.

76. Stamatopoulos D. et al. Exploring the Architectural Composition of Cyber Ranges: A Systematic Review // Future Internet. 2024. № 16(7). P.16. DOI:10.3390/fi16070231.

77. Yamin, M., Katt, B., Gkioulos, V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture // Computers & Security. 2019. V. 88. P. 101636. DOI: 10.1016/j.cose.2019.101636.

78. Macák, M., Oslejsek, R., Buhnova, B. Applying process discovery to cybersecurity training: an experience report //2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2022. Pp. 394-402. DOI:10.1109/EuroSPW55150.2022.00047.

79. Синещук М.Ю. Технические решения по созданию ведомственных организационно-технических систем класса «киберполигон» как средства обеспечения информационной безопасности ведомственного назначения // Научно-аналитический журнал "Вестник Санкт-Петербургского университета ГПС МЧС России". 2024. №.1. С. 179-200. DOI: https://doi.org/10.61260/2218-130X-2024-1-179-20.

80. Матвеев А.В., Синещук М.Ю., Шестаков А.В., Гавкалюк Б.В. Методика технико-экономической оценки вариантов построения организационно-технической системы класса «киберполигон» //Инженерный вестник Дона. 2023. №. 6 (102). С. 187-200.

81. Мистров Л.Е. Модель синтеза систем информационной безопасности организационно-технических систем //Информационная безопасность регионов. 2011. №. 1. С. 21-33.

82. Gerster D. et al. How Enterprises Adopt Agile Forms of Organizational Design: A Multiple-Case Study //ACM SIGMIS Database: the DATABASE for Advances in Information Systems. 2020. V. 51. №. 1. Pp. 84-103. DOI:10.1145/3380799.3380807.

83. Naseir M.A.B. National cybersecurity capacity building framework for counties in a transitional phase: Doctoral Thesis (Doctoral). Bournemouth University, 2020.

84. Pfaller, T. et al. Towards Customized Cyber Exercises using a Process-based Lifecycle Model // EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference: Association for Computing Machinery (ACM), New York, pp. 37-45.

85. Smyrlis M. et al. CYRA: A Model-Driven CYber Range Assurance Platform // Applied Sciences. 2021. V. 11. №. 11. P. 5165. DOI:10.3390/app11115165.

86. Грызунов В.В. Формирование условия гарантированного достижения цели деятельности информационной системой на базе операторного уравнения // Информатизация и связь. 2022. № 4. С. 67-74. DOI 10.34219/2078-8320-2022-13-4-67-74.

87. Ожегов С.И., Шведова Н. Ю. «Ожегов С. И. Толковый словарь русского языка: 72500 слов и 7500 фразеологических выражений». М.: Азъ, 1992. 960 с.

88. Постановление Правительства Российской Федерации «Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» от 12.10.2019 № 1320.

89. Грызунов В.В. Модель целенаправленных агрессивных действий на информационно-вычислительную систему // Человеческий фактор в сложных технических системах и средах (Эрго-2018): Труды Третьей международной научно-практической конференции, Санкт-Петербург, 07 июля 2018 года / Под редакцией А. Н. Анохина, А. А. Обознова, П. И. Падерно, С. Ф. Сергеева. СПб: Межрегиональная общественная организация "Эргономическая ассоциация", 2018. С. 300-305. EDN YUORVZ.

90. Burlov, V.G., Gryzunov, V. V., Tatarnikova, T.M. Threats of information security in the application of GIS in the interests of the digital economy // Journal of Physics: Conference Series : 23 (St. Petersburg, 27–29.05.2020). St. Petersburg: IOP Publishing Ltd, 2020. P. 012023. DOI: 10.1088/1742-6596/1703/1/012023.

91. Грызунов В. В. Методика решения измерительных и вычислительных задач в условиях деградации информационно-вычислительной системы // Вестник СибГУТИ. 2015. № 1(29). С. 35-46. EDN TYYXHR.

92. Цыпкин Я. З. Основы теории автоматических систем: учеб. пособие для вузов. М.: Наука, 1977. 560 с.

93. Калинин В.Н. Теоретические основы системных исследований: краткий авторский курс лекций для адъюнктов академии. СПб: ВКА им. А.Ф. Можайского, 2011. 278 с.

94. Растригин Л.А. Адаптация сложных систем. Рига: Зинатне, 1981. 375 с.

95. Грызунов В.В. Адаптивное управление доступностью ресурсов геоинформационной системы критического применения в условиях деструктивных воздействий: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени доктора технических наук. СПб, 2022. 395 с. EDN SNIOYW.

96. Грызунов В.В., Гришечко А.А., Сипович Д.Е. Выбор наиболее опасных уязвимостей для перспективных информационных систем критического применения // Вопросы кибербезопасности. 2022. № 1(47). С. 66-75. DOI 10.21681/2311-3456-2022-1-66-75. EDN SSVFRQ.

97. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2022, no. 1, pp. 19–29. doi:10.31799/1684-8853-2022-1-19-29.

98. Грызунов В.В. Концептуальная модель адаптивного управления геоинформационной системой в условиях дестабилизации // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1. С. 102-108. EDN GVCRHF.

99. Зализнюк А.Н., Присяжнюк С.П. Стратегическое планирование геоинформационного обеспечения систем управления // Информация и космос. 2016. №3. С.130-132.

100. Зегжда Д.П. Лаврова Д.С., Павленко Е.Ю. Управление динамической инфраструктурой сложных систем в условиях целенаправленных кибератак // Известия РАН. Теория и системы управления. 2020. №3. С.50-63. DOI: 10.31857/S0002338820020134.

101. Кузнецова А. П., Монахов Ю.М. Постановка задачи адаптивного управления очередями для повышения доступности узлов в сетях TCP/IP с частыми потерями кадров // Перспективные технологии в средствах передачи информации-ПТСПИ-2019. 2019. С. 75-78.

102. Грызунов В.В., Романова Н.Н. Способы получения из открытых источников данных о телефоне и аккаунтах пользователя // В сборнике: Цифровые системы и модели: теория и практика проектирования, разработки и применения. Материалы национальной (с международным участием) научно-практической конференции. Казань, 2024. С. 1363-1366.

103. Грызунов В.В., Шестаков А.В., Крюков А.С., Зикратов И.А. Обеспечение информационной безопасности интегрируемых информационных систем на базе доверия // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 110-125. https://doi.org/10.31854/1813-324X-2024-10-4-110-125.

104. Тананко И.Е., Фокина Н.П. Метод анализа сетей массового обслуживания с ненадежными приборами и задержкой информации // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2020. № 52. С. 90-97. DOI: 10.17223/19988605/52/11

105. Нестационарная сетевая модель управляющего аппаратно-программного комплекса / В. П. Бубнов, В. А. Ходаковский, С. А.Сергеев, В. Г. Соловьева // Автоматика на транспорте. 2018. Т. 4, № 2. С. 208–222.

106. Бубнов В.П., Сафонов В.И., Шардаков К.С. Обзор существующих моделей нестационарных систем обслуживания и методов их расчета // Системы управления, связи и безопасности. 2020. № 3. С. 65–121.

107. Федосенко М.Ю. Анализ потенциальных угроз информационной безопасности компьютерной инфраструктуры предприятия в результате осуществления стеганографичских атак // Экономика и качество систем связи. 2024. № 3 (33). С. 146-156.

108. ГОСТ Р 53113.1-2008 Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов.

109. Коржик В.И., Красов А.В. Цифровая стеганография: учебник. Москва: КНОРУС, 2023. 324 с. EDN: KNKBXU.

110. Атакищев О.И., Грибунин В.Г., Комаров И.Д., Борисенко А.Ю., Ермакова Ю.С. Методика обеспечения информационной безопасности автоматизированных систем военного назначения на основе оптимальной достоверности стеганографического анализа передаваемой информации // Известия института инженерной физики. №2 (72). 2024. С.79-85.

111. Красов А.В. Модель нарушителя информационной безопасности, использующего методы стеганографии // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. Санкт-Петербург, 2022. С. 589-592.

CONCEPT, METHODOLOGY, AND TECHNOLOGY FOR BUILDING AND OPERATING AN INTEGRATED CONTINUOUS EDUCATIONAL ENVIRONMENT FOR INFORMATION SECURITY AND INFORMATION PROTECTION INTEGRATED WITH THE INFORMATION INFRASTRUCTURE OF THE EMERCOM OF RUSSIA

Abstract

The article presents the conceptual provisions, methodology, and technology for building and operating a continuous educational environment for information security and information protection, which is integrated with the information infrastructure of the Russian Ministry of Emergency Situations, in order to improve the professional competencies of officials and specialists in the field of information protection.

The materials are intended for managers and specialists who organize educational activities in the field of information security and information protection for the benefit of state and corporate information infrastructures.

The materials were developed based on the results of applied research conducted by the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia in 2024-2025.

Keywords: concept, methodology, technology, continuous educational environment, information security, cyber environment.